Reference	EOP/ESG/DPP/01 Version: June 2, 2021
Policy Title	Data Privacy Policy
Entity	Embassy Office Parks Management Services Private Limited ("**Manager**") in its capacity as the manager of Embassy Office Parks REIT.

Revision History		
Version #	**Version Date**	**Change Type**
V1	April 29, 2021	Reviewed
V2	June 2, 2021	Amended

Document Review Cycle			
#	**Effective Date**	**Next review date**	**Policy Owner**
1	June 2, 2021	On or before May 30, 2022	Chief Executive Officer

Applicability	• This policy is applicable to the Manager, Embassy REIT, its SPVs and its Holdco collectively referred to as "Embassy REIT Entities", and individually as a "Embassy REIT Entity", in this document. • This policy applies to all REIT Entities employees, consultants, interns, contract workers, associates, and temporary employees. • This policy covers all activities where the REIT Entities and its employees collect, store, transfer, use or otherwise process Personal Data of individual persons – notably employees, customers, suppliers, or other contractual and business partners – automatically in full or in part (e.g., by means of electronic data processing). • This policy also applies to non-automated processing if Personal Data is or is intended to be stored in a structured collection, which is available according to specific criteria (e.g., in personnel or customer files), or if Personal data was extracted from an electronic file. This policy also applies to all suppliers and vendors who receive Personal Data from the REIT Entities, have access to Personal Data collected or processed by the REIT Entities, regardless of geographic location. • This policy may be supplemented with alternative or additional policies or implementation procedures applicable in those jurisdictions with unique

	requirements; supplemental or additional policies require approval by the Head of IT, or such other officer as may be designated from time to time. • All partner firms and any Third-Party working with or for REIT Entities, and who have or may have access to personal information or Personal Data, will be expected to have read, understood and provided with a copy of this policy. The REIT Entities shall make best efforts to ensure that such third parties agree to comply with applicable provisions of this policy. The Manager/REIT Entity may require third parties to enter into a confidentiality agreement prior to accessing personal information or Personal Data held by the organization.
Background and purpose of the policy	The Company is committed to complying with the applicable Data Privacy and security requirements in the countries in which it and its subsidiaries operate. Because of differences among these jurisdictions, this Data Privacy Policy creates a common core of values, guidance and procedures intended to achieve compliance. This policy provides a framework for the management of personal data and defines a set of minimum requirements with which the REIT Entities' employees must comply to protect the confidentiality, integrity, availability, and authenticity of the information.
Responsibility for Compliance	The CEO is the policy owner of the Data Privacy Policy and Procedure and responsible for maintaining compliance to the policy and procedures. EMBASSY's Data Privacy program will be overseen by individuals with significant authority and independence. The Company has established a Corporate Data Privacy Officer (**CDPO**). Any queries regarding the implementation of this Policy shall be directed to the Corporate Data Privacy Officer. This policy shall be reviewed for updates by Corporate Data Privacy Officer on an annual basis. Additionally, the data privacy policy may be updated in-line with any on recommendations provided by internal/ external auditors.
Effective Date	The policy is effective from April 1, 2021.
Definitions	**Personal Data and Sensitive Data** • **Personal Data** means data related to a living individual who can be identified from those data or from those data and other information in the possession of, or likely to come into the possession of, a Data Controller or Data Processor. • Personal Identifiable Data is any information that can be used to distinguish or trace an individual 's identity. • any other information that is linked or linkable to an individual ○ **Personal Data may include:** a) Full name

b) Home address

c) Email address

d) Date of Birth

e) Marital status

f) Age

g) Citizenship

h) National Identification Numbers (PAN, Aadhar, Passport etc.)

i) Health

j) Salary

k) Bank account

l) log files

m) or any other personally identifiable information

- **Sensitive Data** means Personal Data relating to the Data Subject's intimate sphere or that might have a significant impact on him/her, such as:

a) Password

b) Race or ethnic origin;

c) Religious beliefs or other beliefs of a similar nature;

d) Political opinions;

e) Physical or mental health or condition including genetic data;

f) Sexual history or orientation;

g) Trade union membership;

h) Biometric information and templates

i) Commission or alleged commission of any offense and any related court proceedings.

j) any detail relating to the above clauses as provided to Embassy for providing service; and

k) any of the information received under above clauses by Embassy for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Additional Definitions

- **Anonymization or de-identification of Personal Data** means that all identifying information (e.g., name, e-mail address, user ID) is redacted to the extent required to ensure that the identity of the Data Subject cannot be determined, or can only be determined with a disproportionate effort.

- **Commissioned Processing** exists if the EMBASSY Data Controller transferring Personal Data continues to determine the purpose and essential means of the processing (e.g., storage period, access rights) and the Data Recipient only processes the Personal Data on behalf of and in accordance with the instructions of the EMBASSY Data Controller (e.g., the Data Recipient technically provides software, in which Personal Data is processed).

- **Data** as used in this Policy shall mean information which either:

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;

b) is recorded with the intention that it should be processed by means of such equipment;

c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;

d) does not fall within any of the above, but forms part of a readily accessible record covering an individual.

Data therefore includes any digital data by computer or automated equipment, and any manual information which is part of a relevant filing system.

- **Data Controller** means a person who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed. Generally, EMBASSY itself will be the Data Controller, although there may be more than one Data Controller within a group of companies if local or overseas offices, subsidiaries or affiliates within the group enjoy a level of autonomy over the processing of the Personal Data they use.

- **Data Processor** means any person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller.

- **Data Recipient** is the natural or legal person, public authority, agency, or any other body to which the Personal Data is disclosed. The Embassy REIT Entities may, from time to time, disclose and/or transfer the Relevant Individuals' Personal Data to third parties (including but not limited) listed below:

    - Parties to Embassy REIT Entities, affiliate companies/ entities and/or other business associates, IT Administrators & Payroll Processors,

- Embassy REIT Entities' insurers and banks;
- External and internal auditors;
- Medical practitioners appointed by the Embassy REIT Entities;
- Administrator of REIT Entities' mandatory provident fund scheme;
- Third parties, advisors and consultants who are involved in a merger, acquisition, due diligence, fund raise or other transactional or advisory exercise associated with Embassy REIT or any of Embassy REIT Entity.
- External companies or third-party service providers Embassy REIT Entities engages to perform Services on the Embassy REIT Entities' behalf;
- Third Parties providing certain information technology application Development and maintenance and data processing services to enable business operations;
- The applicable regulators, governmental bodies, tax authorities or other industry recognised bodies as required by any applicable law or guidelines of any applicable jurisdiction; and
- To any other party as deemed necessary by Embassy REIT Entities.

- **Data Subject** means the natural person to which Personal data refers. Data Subjects include customers and web users, individuals on contact /e-mailing lists or marketing databases, employees (including those of contractors and suppliers).
- **Opt-in** refers to a system whereby Data Controllers obtain specific consent from the Data Subject before the Data Subject's personal information is processed or otherwise used for a particular purpose.
- **Processing** covers a wide variety of operations relating to data, including obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including:

a) Organization, adaptation, or alteration;

b) Disclosure by transmission, dissemination, or otherwise; and

c) Alignment, combination, blocking, erasure, or destruction.

- **Relevant Filing System** means any set of information relating to individuals, whether kept in manual or electronic files, structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Therefore, any digital database and/or organized manual files relating to identifiable living individuals fall within the scope of Data Privacy laws and regulations, while a database of pure statistical or financial information (which cannot either directly or

	indirectly be related to any identifiable living individuals) will not. • **Technology** is to be interpreted broadly, to include any means of collecting, storing or processing Data, including, without limitations, computers and networks, telecommunications systems, video and audio recording devices, databases and data warehouses, biometric devices, closed circuit television, etc. • **Employee** means the current or former employees of the Embassy REIT Entities. As far as it applies to Employees, the Policy covers all stages of the employment cycle including recruitment and selection, promotion, evaluation and training. • **Third Party** means any parties associated with REIT Entities other than its employees or any other internal stakeholders of REIT Entities. • **Consent** means "any freely given specific and informed indication of his wishes by which the Data Subject signifies agreement to Personal Data relating to him being processed." The word "signifies" means that there must be some active communication between the parties. Thus, a mere non-response to a communication from EMBASSY cannot constitute consent. For purposes of EMBASSY's compliance, and in the interest of a consistent approach, EMBASSY will follow the "opt-in" form of affirmative consent. These may include clauses in employment contracts, check boxes on replies to application or purchase forms, and click boxes on online forms where Personal Data is entered. Consent is limited to the specific purposes disclosed to the individual. Further notification and consent is required for new processing activities that extend beyond those for which consent was originally obtained. In the context of new data aggregating activities for which consent had not previously been obtained, additional consent is required. Thus, if data that were collected under an original consent is later aggregated with other data for purposes of transferring the aggregated data to recipients and/or overseas, the original consent likely did not cover this latter activity, requiring additional consent specific to the new uses of the data. The Data Subject's consent must be communicated to Embassy REIT Entities before any processing can take place ("opt-in" approach) and must be revocable.
Focus Areas	**Processing of Personal Data** The Manager has adopted the following principles to govern its processing of Personal Data, or as required by applicable laws: • In processing Personal Data, the individual rights of the Data Subjects must be protected. Data must be processed fairly and in accordance with legal provisions. • Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes. Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they

are collected and/or processed.

- Personal Data shall be accurate, complete and current as appropriate to the purposes for which they are collected and/or processed.
- Personal Data shall not be kept in a form which permits identification of the Data Subject for longer than necessary for the permitted purposes.
- Personal Data shall not be collected or processed unless:

a) processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

b) processing is necessary for compliance with an EMBASSY legal obligation;

c) processing is necessary in order to protect the vital interests of the Data Subject;

d) processing is necessary and/or to potentially improve the experience for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller or in a Recipient to whom the data are disclosed;

e) processing is necessary for legitimate interests of EMBASSY or the Recipient, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject or

f) the Data Subject has provided a valid, informed consent.

- Personal Data shall be collected and processed in accordance with the rights of the Data Subjects.
- Appropriate physical, technical, and procedural controls shall be taken to: prevent and/or to identify unauthorized or unlawful collection, processing, or transmittal of Personal Data; and prevent accidental loss or destruction of, or damage to, Personal Data.
- Processing of personal data is further permitted, if the Data Subject has consented. To be valid, consent must be informed, express, and freely given. If consent is obtained with other written declarations, the request for consent must be made conspicuous.

Sensitive Data Processing

Sensitive Data should not be processed unless:

- Such processing is specifically authorized or required by law.
- The Data Subject expressly consents.
- The processing is required for preventive medicine, medical diagnosis, or health care treatment; provided the data are processed by a health professional subject to national law or rules with an obligation of professional secrecy or by another person with an equivalent obligation

of secrecy. If the Embassy REIT Entities is relying upon this medical exemption, all contracts with employees and independent contractors who will have access to the Sensitive Data must contain confidentiality requirements equivalent to those imposed on health professionals or

- Where the Data Subject is physically or legally incapable of giving consent, but the processing is necessary to protect a vital interest of the Data Subject. This exemption may apply, for example, where emergency medical care is needed.
- Sensitive Data relating to criminal offenses may be processed only by or under the control of an official authority.
- If the Embassy REIT Entities is relying upon one of the exemptions to authorize processing of Sensitive Data, the exemption relied upon, and the basis for the exemptions should be recorded with the data. Any processing of sensitive Personal Data not needed for the proper business operations of EMBASSY must be terminated.

Data Transfers to Recipients

- Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to maintain the required level of Data Privacy. Each entity other than the one that has data to be transferred, shall in terms of this policy be regarded as a Recipient.
- Personal Data may be communicated to Recipients only for reasons consistent with the purposes for which the data were originally collected or other purposes authorized by law. All Personal Data transferred outside of the Embassy REIT Entities or across public communications networks shall be subject to adequate security controls in order to keep its confidentiality.
- A Data Processor processes personal data on behalf of Embassy. All transfers of Personal Data to a Data Processor for further processing shall be subject to prior, written agreements, which shall guarantee a sufficient Data Privacy level. This includes appropriate security controls the Data Processor needs to establish. Where EMBASSY relies on Data Processors to assist in data processing activities (Commissioned Processing), the Embassy REIT Entities will choose a Data Processor who provides sufficient security controls and take reasonable steps to ensure compliance with applicable legislations.
- Any data collected from EU, shall be covered under European Union's General Data Protection Regulation (GDPR), with effect from May 2018.
- EU Personal Data shall not be transferred to a Recipient in a country or territory outside the European Economic Area unless the transfer is made to a country or territory recognized by the EU as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data, or is made in

compliance with one of the mechanisms recognized by the EU as providing adequate protection when transfers are made to countries or territories lacking an adequate level of legal protection.

- Data subjects shall not be required to provide more personal information than is necessary for the provision of the product or service that data subject has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labelled as optional. Collection of personal information shall be avoided or limited when reasonably possible.

- When using vendors to collect personal information on the behalf of Embassy, the Recipient shall ensure that the vendors comply with the privacy requirements of Embassy as defined in this Policy.

- Notwithstanding the above provisions and as a necessary requirement for the transfer of data to another Data Controller, Personal Data may be transferred where any of the following apply:

a) The Data Subject has given consent to the proposed transfer;

b) The transfer is necessary for the performance of a contract between the Data Subject and the Embassy REIT Entities, or the implementation of pre-contractual controls taken in response to the Data Subject's request;

c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Embassy REIT Entities and the recipient;

d) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims;

e) The transfer is required by law;

f) The transfer is necessary in order to protect the vital interests of the Data Subject; or

g) The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

- EMBASSY may conduct assessments on processing by data recipients, especially with respect to their security controls. Embassy shall review the privacy policies and collection methods of Third-Parties before accepting personal information from Third-Party data sources.

New or Expanded Personal Data collection or processing activities

No new or expanded collection or processing activities involving Personal Data may be undertaken without prior information of the CDPO; if Sensitive Data is involved, obtaining approval from the Data Privacy Officer is mandatory.

- To obtain approval, the business unit shall provide the Data Privacy

Officer with the information identified in a data processing assessment form and such other information as the Data Privacy Officer may request.

- The Embassy REIT Entities' Information Technology Department shall establish a procedure for assessing the impact of any new technology uses on the privacy and security of Personal Data. The Information Technology Department shall include such an assessment for each such proposed new or expanded use of technology resources in its application design review process and shall provide such assessments to the Data Privacy Officer.

- All EMBASSY personnel will apply the following guidelines when designing new systems, uses or processes involving Personal Data and/or reviewing or expanding existing activities involving the collection or processing of Personal Data:

a) Collection and use of Personal Data will be avoided or limited when reasonably possible.

b) Personal Data will be anonymized when the purposes of data collection or processing can be at reasonable cost achieved without maintaining personal identification.

c) The purpose(s) of the collecting or processing of Personal Data will be expressly identified by the business unit preparing any new or expanded data collection and processing activity or function.

d) Personal Data may only be used for the purposes for which they were originally collected, or legally mandated purposes, unless the Data Subject has given consent or an exception.

Disclosures at the Time of Data Collection

- Appropriate disclosures will be made at the time a Data Subject is asked to give consent to the collection or processing of Personal Data; and whenever Personal Data are collected. Specific information must be disclosed to the Data Subject and/or any other person from whom Personal Data are obtained at the time of collection unless the Data Subject already has the information. The business unit collecting the information, in cooperation with the CDPO, must establish technical or administrative means for documenting the fact that the Data Subject already has the information and how. The foregoing disclosure requirements shall not apply where such disclosure could not be implemented in a reasonable manner with cost and effort proportionate to the importance of the proposed processing, or where applicable law provides an exemption to requirements for disclosure and/or consent. If no exemption applies, the following information must be disclosed to the Data Subject and/or any other person from whom Personal Data are obtained at the time of collection:

a) The name and address of the Data Controller and, if one has been appointed, the name and address of the Data Controller's representative

for Data Privacy.

b) The purpose(s) of collecting, processing, and transmitting the data.

c) Whether the source of the data is under an obligation to supply the data and the consequences of failing to do so.

d) The identities, or at least the categories, of natural or legal persons who will or may receive the data.

e) Whether any transfers of data outside of the European Economic Area may be made to a country which has not been determined by the EU to have adequate Data Privacy laws.

f) The Data Subject's right to access, receives a copy of, erase, and corrects the data and the means of exercising those rights.

g) How long EMBASSY expects or intends the Personal Data to be retained.

h) Any other information necessary to guarantee "fair processing". For example, where the data are to be used in a manner not apparent to the Data Subject, such use should be disclosed.

- These disclosures should be given as soon as possible and preferably at the first point of contact with the Data Subject. In the case of employees, the disclosures should be made in the employment contract (where reasonable and applicable). Appropriate disclosures should also be made in any job application form or employee handbook.
- The disclosures may be given orally, electronically, via the Embassy REIT Entities' intranet or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Office of Data Privacy. The receipt or form should be retained along with a contemporaneous record establishing the fact, date, content, and method of disclosure.
- If inadequate disclosures are made initially, additional disclosures may have to be made at a later time, and the fact, date, content, and method of these additional disclosures shall be recorded.

Sources of Personal Data

- **Collection of personal data by (Embassy REIT Entities):** Throughout the course of the relationship with the Relevant Individual, (Embassy REIT Entities) needs to collect Personal Data. The type of Information that may be collected includes (but is not limited to), where relevant:

i. Basic Information regarding the Relevant Individuals such as name, contact details, address, gender, birth date, marital status, children, parents details, dependent details, photos, photo id proof, pan card, passport, voter ID, aadhar card, life insurance nominees/beneficiaries, fingerprint information, emergency contact details, citizenship, visa, work permit details;

	ii. Recruitment, engagement or training records including CVs, applications, notes of interview, applicant references, qualifications, education records, test results (as applicable); iii. Information captured as a part of Information & management information systems for the above mentioned processes & other digitization activities. iv. Information about the Relevant Individual's medical condition – health and sickness records; v. The terms and conditions of employment/engagement, employment contracts with the Embassy REIT Entities and/or previous employer; vi. Performance, conduct and disciplinary records within (Embassy REIT Entities) and/or with previous employers; mobility records generated in the course of employment/work with (Embassy REIT Entities); vii. Information relating to the Relevant Individual's membership with professional associations or trade unions; viii. Leave records (including annual leave, sick leave and maternity leave); ix. Financial Information relating to compensation, bonus, perquisites, pension and benefits, salary, travel expenses, stock options, stock purchase plans, tax rates, taxation, bank account, provident fund account, gratuity, insurance details; x. Information captured as result of monitoring of (Embassy REIT Entities) assets, equipment, network owned and/ or provided by (Embassy REIT Entities); xi. Any other Information as required by (Embassy REIT Entities). • Personal Data shall be collected only from the Data Subject unless the nature of the business purpose necessitates collection of the data from other persons or bodies, collection from the Data Subject would necessitate disproportionate effort, or collection must be accomplished under emergency circumstances in order to protect an interest of the Data Subject or to prevent serious loss or injury to another person. • If Personal Data are collected from someone other than the Data Subject, the Data Subject must be informed of the following items unless the Data Subject has received the required information by other means, notification would require disproportionate effort, or the law expressly provides for collection, processing or transfer of the Personal Data: a) The fact of the collection, processing or transfer of the data by the Data Controller; b) The nature and purposes of the processing; c) The recipients or categories of recipients of the data;

d) The origin of the data; and

e) The business unit, in cooperation with the Office of Data Privacy, will create a form or system to document and automate this process as fully as possible.

- Notification to a Data Subject should occur promptly, but in no event later than three months from the first collection or recording of the Personal Data by the Embassy REIT Entities.

Data Subject Rights

EMBASSY acknowledges the rights of each individual to be aware and to be in control of their personal data. The assertion of these rights is to be processed directly by the responsible department. Department responsibility is determined by ownership of the application, which processes the Data Subject`s requested data. If several departments are involved, a representative from the Data Subject`s respective Human Resource department shall coordinate the efforts. Every data subject has the following rights:

a. The data subject may request information on which personal data relating to him/her have been stored, how the data were collected, and for what purpose.

b. If Personal Data are transmitted to Data Recipients, the data subject must also be informed of the recipient's identity, or of the category of recipients.

c. If Personal Data are incorrect or incomplete, the data subject may request for them to be corrected.

d. The data subject may request his/her data to be deleted (if technical possible and/or with reasonable effort, otherwise ensure blocking from any user) if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing archival requirements must be observed.

e. The data subject may object to his/her personal data being used for purposes of market research, or opinion research. Access to the data for these purposes must then be blocked.

f. The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

Data Quality Assurance

- Each employee shall ensure that Personal Data is complete and accurate in the first instance. Data must be accurate and updated in such a way as to give a true picture of the current situation of the Data Subject.

- Employees shall correct data which they know to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification. Inaccurate data must be erased and replaced by corrected or supplemented data.
- Personal Data must be kept only for the period necessary for permitted uses.
- Personal Data should be blocked.

Retention of deletion of personal data

- It is (Embassy REIT Entities)'s policy to retain certain Personal Data of the Relevant Individuals when they cease to be employed/ engaged by (Embassy REIT Entities). This Personal Data may be required for (Embassy REIT Entities)'s legal and business purposes, including any residual activities relating to the employment/engagement, including for example, provision of references, processing of applications for re-employment/re-engagement, matters relating to retirement benefits (if applicable) and allowing (Embassy REIT Entities) to fulfil any of its contractual or statutory obligations.
- All Personal Data of the Relevant Individuals may be retained for periods as prescribed under law or as per (Embassy REIT Entities) policy from the date the Relevant Individuals cease to be employed/engaged by (Embassy REIT Entities). The Personal Data may be retained for a longer period if there is a subsisting reason that obliges (Embassy REIT Entities) to do so, or the Personal Data is necessary for (Embassy REIT Entities) to fulfil contractual or legal obligations. Once (Embassy REIT Entities) no longer requires the Personal Data, it is destroyed appropriately and securely or anonymized in accordance with the law.

Embassy shall perform an internal audit on an annual basis to ensure that personal information collected is used, retained and disposed-off in compliance with the organization's data privacy policy.

Notification to Data Privacy Authorities

EMBASSY shall not process Personal Data without notification to the Data Privacy authorities in jurisdictions which require such notification. The CDPO will always ensure keeping the notifications up to date.

Use of Third-Party Data Processors

- Where EMBASSY relies on third parties to assist in its processing activities, the Embassy REIT Entities will choose a third party who provides sufficient security measures and take reasonable steps to ensure compliance with those measures.
- When using a third party, EMBASSY shall enter into a written contract with each data processor requiring it to comply with data privacy and security requirements imposed on EMBASSY under local legislation.

The contract must also regulate audits of the Data Processor in respect of processing to be carried out by the Data Processor.

- As part of EMBASSY's internal data auditing process, EMBASSY shall conduct regular checks on processing by third party data processors, especially with regard to security controls.
- Obligations for Sub-processor: Where a processor (vendor or 3rd party acting on behalf of Embassy's data processor) engages another processor (Sub-processor) for carrying out specific processing activities on behalf of Embassy (controller), the same data protection obligations as set out in the contract or other legal act between Embassy and the processor shall be imposed on the Sub-processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of GDPR. Where the Sub-processor fails to fulfil its data protection obligations, the initial processor (relevant vendor or 3rd party acting on behalf of Embassy's data processor) shall remain fully liable to Embassy for the performance of that Sub-processor's obligations.

Data Protection Officer – Grievance Officer

- Any questions, discrepancies, and grievances of the Relevant Individuals with respect to processing of Personal Data may be made to the Data Protection Officer (Grievance Officer), herein the Compliance Officer of Embassy Office Parks Management Services Private Limited at "compliance@embassyoficeparks.com" whose name and contact details are available on: https://www.embassyofficeparks.com/investors/resources/#contact-form.
- The Grievance Officer shall redress the grievances of the Relevant Individuals expeditiously and in any event within the period prescribed under law. In case of any queries regarding the content, interpretation, implications of this Policy/ Binding Corporate Rules, the Relevant Individuals may contact the Grievance Officer.

Notwithstanding the above, Embassy REIT Entities reserves the right to decline to process any such request which may jeopardize the security and confidentiality of the Personal Data of others, as well as requests which are impractical or not made in good faith, or the circumstances as provided for under the law permitting Embassy REIT Entities to refuse such request(s).

Employee/ Relevant Individual obligations and consequences of violations

Every Employee/ Relevant Individual, who deals with or comes into contact with Personal Data regardless of its origin (EU or non-EU originated data), shall have a responsibility to comply with the applicable law concerning data privacy, this Policy, the BCRs and specific privacy practices. The Employee/Relevant Individual should seek advice in the event of any ambiguity while dealing with

	Personal Data or in understanding this Policy and the BCRs. The Employee/Relevant Individual shall be diligent and extend caution while dealing with Personal Data of others, in the course of performance of his/ her duties and shall also, at all times: • Prevent any un-authorized person from having access to any computer systems processing Personal Data, and especially: ○ un-authorized reading, copying, alteration, deletion or removal of data; ○ un-authorized data input, disclosure, uploading, transmission/transfer of Personal Data; • Abide by Embassy REIT Entities internal logical and physical security policies and procedures; • Ensure that authorized users of a data-processing system can access only the Personal Data to which their access right refers; • Keep a record of which personal data have been communicated, when and to whom; Not provide any Personal Data to any third party without first consulting with his/her Manager or the Human Resources Department; • Ensure that Personal Data processed on behalf of a third party (client) can be processed only in the manner prescribed by such third party; • Ensure that, during communication of Personal Data and transfer of storage media, the data cannot be read, copied or erased without authorization; • Immediately, on becoming aware report and notify any vulnerabilities and privacy related breach/security breaches (including potential risks). • Attend mandatory and voluntary trainings on security and data privacy including e-learnings and online sessions Failure to comply with the Policy and applicable laws may have serious consequences and can expose both Embassy REIT Entities and the Employee/Relevant Individual to damages, criminal fines and penalties. It is important to note that any non-compliance with this Policy is taken very seriously by Embassy REIT Entities and may lead to initiation of appropriate disciplinary actions including but not limited to Employee dismissal or Relevant Individual termination.
Data Security	**Physical, Technical and Organizational Security Controls** The Embassy REIT Entities shall adopt physical, technical, and organizational controls to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorized processing or access, having regard to the state of the art, the nature of the data, and the risks to which they are exposed by virtue of human action or the physical or natural environment. Adequate security controls should include the following as applicable:

a. Physical Access Control: Prevention of unauthorized persons from gaining physical access to data processing systems in which Personal Data are processed

b. Logical Access Control: Prevention of data processing systems from being used by unauthorized persons.

c. Data Access Control: Preventing persons entitled to use a data processing system from accessing data beyond their needs and authorizations. This includes preventing unauthorized reading, copying, modifying or removal during processing and use.

d. Disclosure Control: Ensuring that Personal Data in the course of electronic transmission during transport or during storage on a data carrier cannot be read, copied, modified or removed without authorization

e. Input Control: Ensuring that it can be subsequently checked and established whether and by whom Personal Data have been entered into, modified on or removed from data processing systems.

f. Control of Processing Instructions: Ensuring that in the case of commissioned processing of Personal Data, the data can be processed only in accordance with the instructions of the Data Controller.

g. Availability Control: Ensuring that Personal Data are protected against undesired destruction or loss.

h. Separation Control: Ensuring that data collected for different purposes can and will be processed separately.

i. Retention Control: Ensuring that data are not kept longer than necessary, including by requiring that data transferred to Data Recipients be returned or destroyed.

Employee Confidentiality

All persons involved in any stage of processing Personal Data should explicitly be made subject to a requirement of confidentiality which should continue after the end of the employment relationship.

Special Rules for Specific Countries

This Data Privacy Policy is designed to provide a uniform minimum compliant standard for every entity with respect to its protection of Personal Data worldwide. EMBASSY recognizes that for some part of this document certain laws may require stricter standards than those described in this Policy. With prior approval of Data Privacy Officer, only for the specific part in conflict, those entities will handle Personal Data in accordance with local law applicable at the place where the Personal Data are processed; the rest of the document remains in effect.

	Compliance Compliance with Data Privacy laws, protection of personal and sensitive data, and the requirements specified in this policy are the responsibility of every Employee. Each Employee is responsible for acquiring a sufficient understanding of this AS and to comply with the requirements specified herein. Any breach of this policy will be regarded as a serious matter by the Embassy REIT Entities and may result in disciplinary action / sanction up to and including termination of employment. The CDPO shall notify the Audit Committee that: failure to comply with relevant Data Privacy legislation may trigger criminal and civil liability, including fines, imprisonment, and damage awards; and they can be personally liable where an offense is committed by EMBASSY with their consent or connivance, or is attributable to any neglect on their part. **Controls** Adequate controls and Key Performance Indicators, to measure the efficiency of this policy shall be defined by the Corporate Data Privacy Officer and described in additional guidelines. The Audit Committee will review those controls at least on a yearly basis.
References to applicable Acts	The Personal Data Protection Bill (when enforced); General Data Protection Regulation (GDPR); Information Technology Act, 2000 (also known as ITA-2000, or the IT Act); The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.
Amendment	This policy will stand automatically amended to the extent of any relevant change(s) in the applicable law and or for any change(s) in fact.