Client Due Diligence Privacy Notice

Last Updated: [01.01.2026]
Last Reviewed: [01.01.2026]

This CBRE Client Due Diligence Privacy Notice ("**Notice**") is issued by CBRE Limited and its subsidiaries ("**CBRE**"), excluding CBRE Caledon Holdings, to assist you in understanding our data collection and handling practices when you provide CBRE with personal information, which will be used to complete regulatory and client due diligence background checks.

This Notice is also intended to assist you in making informed decisions and exercising your data privacy rights under applicable law.

Whenever this Notice refers to "CBRE", "we", "us" or "our", it refers to the applicable responsible CBRE Group entity/ies defined in Appendix 1 below.

Table of Contents

Summary of Key Information

SCOPE	This Notice applies to the personal information provided to CBRE for the purpose of completing regulatory and client due diligence checks as required in relation to: • when acting as an agent in a purchase, sale, or lease of real property or immovables: • servicing mortgage agreements on real property or hypothecs on immovables on behalf of lenders: • to act as an intermediary between a lender and a borrower for loans secured by mortgages or hypothecs. • engaged in providing loans secured by mortgages or hypothecs.

RESPONSIBLE ENTITY / DATA CONTROLLER	CBRE [Entity] is the data controller/responsible entity. Please find information on how to identify your applicable responsible CBRE entity (or entities) in Appendix 1. See details below in Information about the Responsible CBRE Entity / Data Controller.
PERSONAL INFORMATION WE COLLECT / SOURCES	We collect the following categories of personal information directly from you, from your employer/the organization you represent or with which you are associated, and from our third-party due diligence service providers: • Basic data • Business Contact and Employment Information • Financial or tax information • Criminal convictions or offenses information • Special categories of data • Compliance data See details below in Personal Information We Collect and Sources.
SPECIAL CATEGORY / SENSITIVE PERSONAL INFORMATION WE COLLECT	Where we may lawfully do so under applicable law, as part of our regulatory check and client due diligence activities, we may also collect information (also known as special category or sensitive personal information in some jurisdictions) **("Sensitive Data")** including information about criminal convictions and offenses and/or information about your affiliation with, or membership in, any group, party, or organization of a political nature insofar as such affiliation or membership is indicative that you may be a "Politically Exposed Person". See details below in Personal Information We Collect and Sources.
USE OF YOUR PERSONAL INFORMATION AND LEGAL BASES	We use your personal information to complete our legally required regulatory and client due diligence background checks. We carry out such processing based on our legal obligations with respect to investor due diligence, to communicate with you and facilitate your entry into a subscription agreement with CBRE, and/or based on your consent. See details below in Use of Personal Data.
DATA SHARING	We share your personal information internally with other CBRE entities as it may be necessary to complete our regulatory check and client due diligence activities, and with our service providers, insurers, brokers, and/or loss adjusters, consultants and advisors, third-party due diligence service providers, business partners in the event of a merger or sale, and governmental regulators. See details below in Sharing of Personal Data.

DATA RETENTION	We retain the personal information we collect about you for as long as necessary for the purpose for which that information was collected or as otherwise legally required. See details below in Retention of Personal Data.
DATA SECURITY	We implement appropriate technical and organizational security measures to safeguard the personal information we collect and process about you against loss and unauthorized alteration or disclosure. See details below in How We Secure Your Personal Information.
INTERNATIONAL DATA TRANSFERS	We may share your personal information with other CBRE entities and service providers located outside of your country of residence. When doing so, we provide appropriate safeguards for international data transfers as required by applicable law. See details below in International Data Transfers.
PRIVACY RIGHTS	Depending on the laws in your country, you may have certain rights to request access, rectification, deletion, objection, or other actions regarding your personal information. See details below, including how to exercise any privacy rights you may have under applicable law, in Your Data Privacy Rights.
CONTACT CBRE	You are always free to contact us if you have questions or concerns about this Notice or our personal information collection and processing activities. See details below in Contact CBRE.
DATA PROTECTION OFFICER	Where required by law, we have appointed a Data Protection Officer, whose contact details are disclosed in this Notice. Click here to learn more.
EU/UK REPRESENTATIVE	We have appointed a representative for any responsible CBRE entity located outside of the EEA and the UK that processes personal information subject to the EU General Data Protection Regulation and UK data protection law. Click here to learn more.
CHANGES TO THIS NOTICE	If we make any material changes to this Notice, we will make changes here and, if the changes are significant, we will provide a more prominent notice. Where required, we will obtain your consent. See details below in Changes to this Notice.

Full Notice

1. Information About the Responsible CBRE Entity / Data Controller

Depending on the legal regulations in your country and the applicable laws to which you are subject (such as in the EU/EEA and UK), you may have the right to information on the CBRE entity (or entities) responsible for collecting and processing your personal information (also known as the data controller in some jurisdictions). CBRE is the data controller/responsible party. Information on how to identify your applicable responsible CBRE entity (or entities) is in Appendix 1.

2. Personal Information We Collect and Sources

a. Categories of Personal Information We Collect

Where we may lawfully do so under applicable law, we collect the following categories of personal information directly from you or from other sources, such as your employer or the organization you represent or with which you are engaged, and from our third-party due diligence service providers. For more information on data sources, see **Sources from Whom We Collect Personal Information**, below.

Category Number	Category	Examples
1	**Basic data**	Your name, phone number, mailing address, and email address.
2	**Business Contact and Employment Information**	Your name, title, organization/employer, employment history, business telephone number, and business email address
3	**Financial or tax information**	In each case for the current calendar year and for up to three (3) years prior to the current calendar year,: Bank account numbers, transaction history, salary information, personal net worth statement (listing assets, liabilities, and equity), personal credit report, copies of tax returns and/or notices of assessment and related documentation proof of personal income, such as pay stubs, T4/T4A forms (or equivalent in your country of residence) or the equivalent if self-employed, and closed-for-cause banking records.
4	**Criminal convictions or offenses information**	Records of any criminal convictions or offenses you have committed, whether in your country of residence or any other jurisdiction.
5	**Special categories of data**	Affiliation with, or membership in, any group, party, or organization of a political nature, insofar as such affiliation or membership is indicative that you may be a “Politically Exposed Person”.
6	**Compliance data**	Government identifiers, driver’s license number, social insurance number, social security number, national insurance number, federal, provincial, or municipal government identification number, or other applicable national, state, or local government identification number, passport or other government-issued identification documents, dates of birth, beneficial ownership data, and due diligence data.

b. Special Categories of Personal Information

To the extent we may do so under applicable law, we may collect and process categories of personal information relating to you which (depending on the applicable legal regulations and law in to which you are

subject, such as in the EU/EEA and UK) enjoy special protection by qualifying as special categories of personal information, sensitive personal information or similarly. Examples of such special categories of personal information include the Sensitive Data described herein. We will collect and process those categories of personal information only where allowed by law, subject to any restrictions and additional safeguards as required by law and where relevant to and necessary to complete our regulatory check and client due diligence activities as are required under applicable law.

c. Sources From Whom We Collect Personal Information

We collect and process personal information directly from you, from your employer/the organization you represent, and from our third-party due diligence service providers.

d. Consequences of Not Providing Personal Information

CBRE may require certain Personal Information necessary prior to forming or performing contracts with you, and to comply with our legal obligations. If you fail to provide the requested Personal Information, we may be unable to proceed with the transaction.

3. Use of Personal Information and Legal Bases

The purposes for which we use your personal information and the legal base for such processing are as follows:

Purpose Number	Purpose of Processing	Categories of Personal Data Processed	Lawful Bases of Processing
1	To complete the legally required client due diligence checks	(1) Basic data; (2) Business Contact and Employment Information; (3) Financial or tax information; (4) Criminal convictions or offenses information; (5) Special categories of data (6) Compliance data	• Compliance with our legal obligations with respect to performing due diligence on potential investors. • Facilitating our entry into a contract with you. • Consent
2	To communicate with you about the status and/or results of regulatory and client due diligence checks	(1) Basic data; (2) Business Contact and Employment Information	• Facilitating our entry into a contract with you. • Consent
3	To manage our business operations and administer our client relationships	(1) Basic data; (2) Business Contact and Employment Information	• Facilitating the execution of, and performance of our obligations under, a contract with you
4	To establish, exercise or defend our legal rights, to comply with lawful government requests for disclosure of personal information or otherwise to comply with legal obligations	(1) Basic data; (2) Business Contact and Employment Information; (3) Financial or tax information; (4) Criminal convictions or offenses information; (5) Special categories of data; (6) Compliance data	• Compliance with legal obligations • Legitimate interests

a. Legitimate Business Interests

To the extent that CBRE relies on its overriding legitimate business interests for the processing of your personal information, such business interests are establishing, exercising, or defending our legal rights and claims.

To the extent any of the processing purposes listed above require the processing of Special Categories of Information, such processing may in particular be permitted under applicable law as the processing is necessary to carry out certain obligations or exercise certain rights in the field of employment, social security and social protection, to establish, exercise or defend a legal claim, for reasons of substantial public interest or of public interest in the area of public health, and other necessary objectives or based on your consent (if required by law).

b. Automated Decision-Making

CBRE does not process any personal data it collects and processes during the regulatory check/client due diligence process to make automated decisions.

4. Sharing of Personal Information

Where we can do so lawfully under applicable law, the personal information we collect may be shared and processed with the following categories of recipients, some of whom may be located in a country that does not provide an adequate level of data privacy and protection rights as your home country, as necessary for the purposes identified in Section 3 – Use of Personal Information and Legal Bases, above. CBRE has in place appropriate safeguards regarding internal personal information sharing. See International Data Transfers below for more information.

a. Internally with Other CBRE Entities

CBRE is a global firm, and the personal information we collect or you provide may be shared and processed with CBRE entities as necessary for the purposes identified in Section 3 – Use of Personal Information and Legal Bases, above. The potentially relevant CBRE entities are identified in Appendix 1. In particular:

- As part of CBRE's regulatory check and client due diligence activities, CBRE's global matrix structure may require that your personal information (including, Sensitive Data) is transferred to other CBRE entities outside your home country where other CBRE employees who are responsible and accountable for carrying out client due diligence activities and reviewing client due diligence check results are located (e.g., regional or global legal and compliance functions).
- Where legally permissible to process and transfer Sensitive Data outside your home country, and if you provide it, your Sensitive Data may be shared with other CBRE entities outside your home country as is necessary to complete our legally required client due diligence activities. To the extent possible, we will share such data in an aggregated, pseudonymized format.

b. With Third-Parties

The potentially relevant third parties include:

- **Service Providers** who assist us with insurance claims processing and benefits, IT, cyber security, and data hosting providers.
- **Insurers, brokers, and/or loss adjusters** as necessary to file and insurance claims.
- **Consultants and advisors** who assist us with legal, regulatory, and business operations activities, such as legal counsel, compliance consultants, business auditors, and third-party due diligence service providers.
- **Governmental Regulators** as necessary to comply with CBRE's legal obligations in the fields of employment law and occupational health and safety law in certain countries.
- **Lenders** for ongoing servicing and to evaluate creditworthiness, structure financing, and adhere to anti-money laundering and compliance regulations.
- **Business partners in case of a merger or sale**, such as if CBRE is merged with another organization, or in the event of a transfer of our assets or operations.

c. Legally Compelled Disclosure

We may be required to disclose your personal information to governmental and regulatory authorities, law enforcement agencies, courts and/or litigants when legally compelled to do so, for example, in response to a court order, subpoena or other lawful, legally-binding request, including to meet national security or law enforcement agencies requirements, or in connection with legal proceedings or similar processes as necessary to exercise or defend our legal rights.

CBRE is committed to not disclosing your personal information in response to an international court order, a subpoena, or other legal obligation, unless we are legally compelled to do so under applicable law. In particular, CBRE, Inc. has assessed and is of the view that neither it nor its US subsidiaries qualify as a provider of electronic communication service, as defined in 18 U.S.C. § 2510, nor a provider of a remote computing service, as defined in 18 U.S.C. § 2711, and thus US public authorities cannot issue a legally binding demand for disclosure of data under Section 702 of the US Foreign Intelligence Surveillance Act ("**FISA 702**") upon CBRE, Inc. or its US subsidiaries. In case CBRE nevertheless receives at some point a disclosure demand for personal information under FISA 702, we will publish a Transparency Report on cbre.com and our EEA websites (see our Schrems II statement). All personal data transferred by CBRE to the US is encrypted in transit.

5. Retention of Personal Information

We will retain your personal information only for as long as required to satisfy the purpose for which such information was collected, unless otherwise required by law or regulation to be retained for a longer period. Personal information collected as described in this notice will be retained for at least five years in accordance with FINTRAC guidelines. If you require further information as to the retention period, please do not hesitate to contact us.

6. How We Secure Personal Information

We implement appropriate technical and organizational security measures to safeguard the personal information we collect and process about you against loss and unauthorized alteration or disclosure. The information you provide is encrypted in transit and at rest. We utilize role-based access controls to limit access to your personal information on a strict need-to-know basis consistent with the purposes for which we have collected such information. We utilize anti-malware and intrusion detection systems to guard against unauthorized access to our network, and we have an incident response plan in place to quickly respond to any suspected leak or breach of personal information.

When we share your personal information with our service providers, we have assessed that their technical and organizational measures provide an appropriate level of security.

7. International Data Transfers

Depending on the CBRE entity that is the responsible CBRE entity (see Appendix 1 below) and the recipients (see Sharing of Personal Information above), your personal information may be processed and hosted in countries other than your home country, such as the United States. Those other countries may have less stringent data protection laws than the country in which you reside, in which you initially provided the information, and/or in which your information was originally collected.

In the event of international data transfers, we will protect your personal information in accordance with all applicable data protection laws.

a. EEA and UK to Non-EEA Data Transfers

With respect to international data transfers initiated by CBRE from the European Economic Area ("**EEA**") or UK to recipients in any non-EEA jurisdictions,

- some recipients are located in countries that are considered to provide an adequate level of data protection under EU law (or UK law, as applicable). These transfers do not, therefore, require any additional safeguards under EU (or UK, as applicable) data protection law.
- other recipients are located in the U.S. and are certified under the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**") and the UK-U.S. extension to the EU-U.S. DPF ("**UK Extension**"). CBRE has assessed, therefore,

that these transfers do not require any additional safeguards under EU (or UK, as applicable) data protection law. Nonetheless, CBRE has a general practice of executing EU Standard Contractual Clauses and UK Addenda with respect to such transfers to U.S. recipients.

- other recipients are located in countries not providing an adequate level of data protection under EU or UK law, (or, while located in the U.S., have not certified under the EU-U.S. DPF or UK Extension) and, where required by law, we have implemented appropriate safeguards, such as EU Standard Contractual Clauses, and/or are relying on binding corporate rules of the recipient or an appropriate derogation. Where applicable, we implement supplementary technical and contractual safeguards. Under applicable law you may have the right to ask for further information on such appropriate safeguards (see Section 9 - Contact CBRE below).

As stated above (see Legally Compelled Disclosures), CBRE, Inc. has assessed and is of the view that US public authorities cannot issue a lawful disclosure demand for personal data under FISA 702 upon CBRE, Inc. or its US subsidiaries. All personal data transferred by CBRE to the US is encrypted in transit.

b. Data Privacy Framework Program

The EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"), UK Extension to the EU-U.S. DPF ("**UK Extension**"), and Swiss-U.S. DPF ("**Swiss-U.S. DPF**") were respectively developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union, United Kingdom, and Switzerland while ensuring data protection that is consistent with EU, UK, and Swiss law. To learn more about the DPF and to view our certification, please visit https://www.dataprivacyframework.gov/s/participant-search.

CBRE, Inc. complies with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF as set forth by the U.S. Department of Commerce. CBRE, Inc. has certified to the U.S. Department of Commerce that it, and its U.S. entities described below ("**CBRE U.S.**"), adhere to the EU-U.S. Data Privacy Framework Principles ("**EU-U.S. DPF Principles**") with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. CBRE U.S. has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles ("**Swiss-U.S. DPF Principles**") with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern.

The following U.S. subsidiaries of CBRE, Inc. adhere to EU-U.S. DPF Principles and the Swiss-U.S. DPF Principles: CBRE Security Services, Inc; CBRE HMF, Inc.; CBRE Multifamily Capital Inc.; CBRE Capital Markets, Inc.; CBRE Technical Services, LLC; Trammell Crow Company, LLC; CBRE GWS of Puerto Rico, Inc.; CBRE Design Collective, Inc.; Millman Surveying, Inc.; CBRE GWS Licentia, LLC; CBRE Government Services, LLC; CBRE Securities, LLC; CBRE GWS Licentia, LLC; Full Spectrum Group, LLC; FacilitySource, LLC; CBRE GWS, LLC; Cascade Thermal Solutions, LLC; CBRE Managed Services Inc.; CBRE Management Services Inc.; and CBRE Investment Management Listed Real Assets LLC.

The Federal Trade Commission has jurisdiction over CBRE U.S. as it relates to compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

Additionally, this policy adheres to the EU-U.S. DPF Principles with regard to personal data transferred from the European Union and the United Kingdom and the Swiss-U.S. DPF Principles with regard to personal data transferred from Switzerland.

Disclosure and Liability for Onward Transfer

CBRE is required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. CBRE may, as disclosed above in Sharing of Your Personal Information, transfer personal information onward to third parties. CBRE remains liable under the DPF Program if a third party processes such personal information in a manner inconsistent with the DPF Principles, unless we prove we are not responsible for the event giving rise to the damage.

Independent Recourse of DPF Complaints

In compliance with the EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF, CBRE commits to resolving complaints about our collection or use of your personal information. EU, U.K., and Swiss individuals with inquiries or complaints regarding our DPF Program compliance should first contact CBRE at: Privacy.Office@cbre.com.

In the event of unresolved complaints or concerns, CBRE commits to cooperate with respective Data Protection Authorities ("**DPAs**"), including local EU DPAs (and empanelled DPAs) concerning disputes arising from EU individuals, with the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA) concerning disputes arising from UK (and Gibraltar individuals), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) concerning disputes arising from Swiss individuals. CBRE will comply with the advice provided by the respective authorities with regard to unresolved complaints concerning our handling of personal data processed in reliance on the EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. You also have the right to invoke binding arbitration in accordance with the terms set forth in Annex I of the Principles of the EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF.

8. Your Data Privacy Rights

Depending on the legal regulations in your country and the applicable laws to which you are subject, you may have all or some of the following rights set out below and may submit a request(s) to exercise any such rights through our Data Subject Rights Portal or by contacting us at dsr@cbre.com. Irrespective of the CBRE entity that is responsible for the processing of your personal information, you may use such centralized contact details, and CBRE will ensure that the responsible CBRE entity receives your request and addresses it promptly as required by applicable law. CBRE will respond to your request comprehensively, even if you do not identify the particular CBRE entity against whom you make the request.

- **Right of access**: You may have the right to obtain confirmation from CBRE as to whether your personal information is being processed, and, where that is the case, to request access to your personal information. You may have the right to obtain a copy of your personal information that is being processed. For additional copies requested by you, CBRE may charge a reasonable fee based on administrative costs.
- **Right to rectification:** You may have the right to obtain from CBRE the rectification of inaccurate personal information concerning you.
- **Right to erasure (right to be forgotten) or anonymization:** You may have the right to ask us to erase (or, in some jurisdictions, anonymize) your personal information. In some jurisdictions, this right may be limited to deletion or anonymization of data that is unnecessary, excessive, or unlawfully processed, or deletion of data that is processed based on your consent.
- **Right to restriction of processing:** You may have the right to request the restriction of processing your personal information.
- **Right to data portability:** You may have the right to receive your personal information, which you have provided to CBRE, in a structured, commonly used, and machine-readable format, and you may have the right to transmit that personal information to another entity without hindrance.
- **Right to withdraw consent:** If we rely on your consent for any personal information processing activities, you have the right to withdraw or revoke this consent at any time with future effect. Such a withdrawal will not affect the lawfulness of the processing that occurred prior to the withdrawal of consent. This right to withdraw consent applies to consents given for marketing and profiling purposes, if any.

- **Right to object:** Under certain circumstances, you may have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal information by CBRE, and CBRE can be required to no longer process your personal information unless CBRE demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims. The right to object may, in particular, not exist if the processing of your personal information is necessary to take steps prior to entering into a contract or to perform a contract already concluded.

- **Right to request an explanation of our processing of your personal information**
- **Right to information on the possibility of withholding consent** and information on the consequences of doing so**.**
- **Right to information on** third **parties with whom we share your data.**
- **Right to lodge a** complaint **with the competent data protection authority** in your home country or in the country in which the responsible CBRE entity is located, with respect to the result of automated decision-making.

9. California Privacy Policy

If you are a resident of the State of California ("**Consumer**"), CBRE's California Privacy Policy ("**California Policy**") supplements the information provided in this Notice and includes information about your privacy rights and how to exercise them. The California Policy applies solely to personal information we have collected from individuals who are residents of the State of California in the twelve (12) months preceding the date on which the California Policy was last updated.

Depending on how you interact with CBRE, we may collect certain personal information. We collect the

following information about you:

- **Identifiers** such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Any personal information described in subdivision (e) of Section 1798.80 of the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020.
- **Characteristics of protected classifications** under California or federal law.
- **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- **Biometric information**.
- **Internet or other electronic network activity information**, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.
- **Geolocation data**.
- **Audio, electronic, visual, thermal, olfactory, or similar information**.
- **Professional or employment-related information**.
- **Sensitive personal information**.

CBRE uses this information to achieve the purposes outlined in the 3. Use of Personal Information and Legal Bases section above.

10. Contact CBRE

a. You are always free to contact us if you have questions or concerns regarding this Notice or our data handling practices. General Enquiries

You may contact CBRE's Global Data Privacy Office ("**GDPO**") at Privacy.Office@cbre.com or by writing to us at 321 North Clark Street, Suite 3400, Chicago, Illinois 60654, Attention: Global Director, Data Privacy. You may also raise questions or concerns about the GDPO to CBRE's Ethics & Compliance department via the CBRE Ethics Helpline.

Individuals in Europe, the Middle East or Africa:

If you are located in Europe, the Middle East or Africa, you may also e-mail us via the GDPO at EMEAPrivacyDirector@cbre.com or write to us Henrietta House, Henrietta Place, London W1G 0NB, United Kingdom, Attention: EMEA Director, Data Privacy.

Individuals in Asia or the Pacific:

If you are located in Asia or the Pacific, you may also e-mail us via the GDPO at APACPrivacyHelpline@cbre.com or write to us at 15/F M1 Tower, 141 H.V. Dela Costa Street, Salcedo Village, Makati City, Philippines 1227, Attention: APAC Senior Manager, Data Privacy.

b. Data Protection Officers

We have appointed data protection officers ("DPOs") for Responsible CBRE Entities in certain countries in accordance with local law. If you have any questions or concerns about our personal information policies or practices, a list of appointed DPOs and their contact details can be found in our Global Privacy and Cookie Notice.

11. Changes to this Notice

We are a rapidly evolving, global business. We will continue to assess and make changes to this Notice from time to time as required. If we make any material changes to this Notice, we will make changes here and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Notice changes). Where required, we will obtain your consent.

Appendix 1

In the table below, the responsible CBRE entity (also referred to as data controller in some jurisdictions) for personal information have been identified, depending on various factors of the processing activity.

If it is unclear to you which CBRE entity is the responsible CBRE entity for the processing of your personal information, please contact privacy.office@cbre.com, and we will help you identify the responsible CBRE entity.

	Processing Activity	Responsible CBRE Entity / Data Controller
A.	Completing legally required background checks and client due diligence activities.	CBRE Limited 1300 - 1969 UPPER WATER STREET, MCINNES COOPER TOWER - PURDY'S WHARF, HALIFAX, NOVA SCOTIA, B3J 3R7, CANADA is the data controller/responsible entity.