CANARY WHARF GROUP

# CODE OF CONDUCT FOR PERSONAL DATA

Procedure Owner: Data Protection Officer

LEG-P-001

| REVISION / REVIEW HISTORY | | | | |
|---|---|---|---|---|
| Date | Summary of changes | Revision Number | Authored / Revised by | Approved by |
| 03/2024 | First Issue | 00 | A Wickham | A Wickham |

REVIEW PERIOD: 2 YEARS

TABLE OF CONTENTS

## 1. OBJECTIVE AND SCOPE

1.1 This code of conduct describes the obligations and responsibilities in relation to the processing of personal data by all contractors and suppliers of goods or services to Canary Wharf Group plc or any of its subsidiaries or group companies.

1.2 This code of conduct is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Laws.

1.3 This code of conduct and the terms of any Agreement relating to the processing of personal data shall be treated as mutually explanatory of each other. Unless otherwise expressly stated in the Agreement, the Contracting Party's obligations and CWG's rights and remedies under this code of practice are cumulative with, and additional to, any other provisions of the Agreement.

1.4 Without prejudice to 1.3, in the event of conflict or discrepancy between this code of conduct and other express written terms agreed between the parties relating to the processing of personal data, the latter shall take priority.

1.5 Details of the processing activities are set out in the Appendix to this code of practice and may be supplemented by additional specific details contained in the Agreement.

## 2. DEFINITIONS

"Agreement" the purchase order, trade contract, consultant appointment or other contract entered into between CWG and the Contracting Party;

"CWG" means Canary Wharf Group plc or such other CWG company or subsidiary company, special purpose vehicle company incorporated by or on behalf of CWG and any joint venture company in which CW is a partner that has entered into an Agreement;

"Contracting Party" means the relevant trade contractor, consultant, supplier, person or other entity who is providing services pursuant to the Agreement;

"Data Breach" means any breach of security, breach of the laws or breach of obligations or any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any personal data;

"Data Protection Laws" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018;

"Processing End Date" means in respect of any Protected Data, the earlier of (a) the end of the provision of the relevant services related to the processing of such Protected Data or (b) once processing by the Counterparty is no longer required for the purpose of the Counterparty's performance of its relevant obligations under the Agreement.

"Protected Data "means personal data received from or on behalf of CWG or otherwise obtained in connection with the performance of the Counterparty's obligations under the Agreement.

"Sub-Processor" means and processor engaged by the Contracting Party (or by any other sub-processor) for carrying out any processing activities in respect of the Personal Data.

"Trade Contract" means any contract for construction works (including contractor design works) between CWG and a third party.

"Trade Contractor" means any person or entity who is carrying out work pursuant to a Trade Contract.

"UK GDPR" means the General Data Protection Regulation, Regulation (EU) 2016/679 as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom from time to time).

The following terms have the same meaning as set out in the Data Protection Laws: "data controller", "data processor" "data subject"; "personal data" or "data" (used interchangeably), and "processing".

## 3. GENERAL PRINCIPLES

3.1 This code of conduct commits all parties to comply with the following principles and to support and co-operate with other parties in their own compliance:

3.2 Protected Data must be:

3.2.1 Processed lawfully, fairly and in a transparent manner.

3.2.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.2.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.2.4 Accurate and, where applicable, kept up to date; every reasonable step must be taken to ensure that Protected Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

3.2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Protected Data are processed.

3.2.6 Processed in a manner that ensures appropriate security of the Protected Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.3 In order to comply with these principles, the parties must:

3.3.1 Fully implement all appropriate technical and organisational measures to ensure a level of security appropriate to the risk connected with the processing.

3.3.2 Maintain up-to-date and relevant documentation on all processing activities.

3.3.3 Implement measures to ensure privacy by design and default, including:

3.3.3.1 Data minimisation

3.3.3.2 Pseudonymisation

3.3.3.3 Transparency

3.3.4 Allow individuals to exercise their legal rights pursuant to UK GDPR.

3.3.5 Conduct data protection impact assessments where appropriate.

## 4. DATA CONTROLLER & DATA PROCESSOR STATUS

4.1 Save where Data Protection Laws provide otherwise, CWG is the data controller and the Counterparty is the data processor. In these circumstances, only CWG can decide:

4.1.1 the purpose and how Protected Data is used;

4.1.2 what Protected Data to collect and the legal basis for doing so;

4.1.3 which individuals (data subjects) to collect data about;

4.1.4 whether to disclose Protected Data, and if so, who to;

4.1.5 how data subjects' rights apply;

4.1.6 how long to retain the Protected Data; and

4.1.7 whether to make non-routine amendments to the Protected Data.

## 5. COUNTERPARTY'S RESPONSIBILITIES RELATING TO PROTECTED DATA

5.1 When processing Protected Data the Counterparty must:

5.1.1 Only process (and shall ensure Contracting Party personnel only process) the Protected Data in accordance with the Agreement and CWG's written instructions from time to time (including with regard to any transfer to which 5.5.6 relates) and the Appendix to this code of practice, except where otherwise required by applicable law (and in such a case shall inform CWG of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest).

5.1.2 Not break any Data Protection Laws.

5.1.3 Maintain complete, up to date, and accurate records and information to demonstrate its compliance with the Data Protection Laws, which shall include records of its processing activities performed on behalf of CWG and a general description of the security measures implemented in respect of processed data and provide a copy of such records to CWG upon request (see section 6);

5.1.4 Have in place appropriate technical, security and organisational measures to protect the data against loss, destruction, damage, alteration or disclosure (see Appendix Section 2);

5.1.5 Not change, remove or alter the data or share it with any third party without CWG's permission;

5.1.6 Not transfer any Personal Data outside of the UK unless CWG's prior written consent has been obtained and the following conditions are fulfilled by the Counterparty;

5.1.6.1 the provision of appropriate safeguards in relation to the transfer;

5.1.6.2 ensuring any data subjects affected have enforceable rights and effective legal remedies;

5.1.6.3 complying with its obligations under the Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred; and

5.1.6.4 complying with reasonable instructions notified to it in advance by CWG with respect to the processing of the Personal Data;

5.1.7 Keep Protected Data in a manner that can be readily separated and distinguished from any other data it processes;

5.1.8 Make sure that only those staff who need to access Protected Data are granted access to it and that all staff who are provided such access: are reliable and trustworthy; have been trained in data protection; have been told the data is confidential; have signed a duty of confidentiality; and comply with the obligations set out in this code of conduct;

5.1.9 Inform its staff that CWG may process their data, which may include sensitive personal data, including biometrics (where access to restricted areas is required), passport details, right to work and citizenship information and CCTV footage.

5.1.10 Obtain CWG's written permission if it wants to use Sub-Processors to process any Protected Data. If written permission is granted, the Contracting party shall ensure the Sub-Processors shall, at all times, comply with all Data Protection Laws in connection with the processing of Protected Data and the provision of the Services and shall not by any act or omission cause CWG (or any other person) to be in breach of any of the Data Protection Laws;

5.1.11 Notify CWG without delay (and within twenty-four (24) hours) if it has or believes that it has breached any Data Protection Laws or if any data breach occurs or is believed to have occurred;

5.1.12 Notify CWG without delay (and within forty-eight (48) hours) if it receives: any request from a relevant data subject to exercise their rights under Data Protection Laws (e.g. if they make a subject access request); or if it receives a complaint or any communication from the Information Commissioner's Office ("ICO") relating to the manner in which it processes personal data;

5.1.13 Have in place procedures to assist CWG to ensure compliance if a data subject chooses to exercise their rights under the Data Protection Laws;

5.1.14 Allow without charge CWG reasonable access to audit all records, files, tapes, computer systems, or any other information relating to services provided under the Agreement and upon request to provide evidence to CWG's reasonable satisfaction that the Counterparty's obligations relating to Protected Data are being met;

5.1.15 Assist CWG in responding to any request from a Data Subject and in ensuring compliance with CWG's obligations under the Data Protection Laws with respect to security, data breach notifications, impact assessments and consultations with supervisory authorities or regulators;

5.1.16 Tell CWG, if it believes CWG's instructions are unlawful; and

5.1.17 At the completion of the Agreement, or if CWCL asks it to, the Counterparty shall (and shall ensure that each of the Sub-Processors and Counterparty personnel shall) within not less than 5 business days and not more than 7 business days of the relevant Processing End Date at CWG's discretion return or securely delete the Protected Data (and all copies) except to the extent that storage of any such data is required by applicable law (and, if so, the Supplier shall inform CWG of any such requirement and shall securely delete such data as soon as it is permitted to do so under applicable law.

## 6. RECORDS

6.1 In relation to all Protected Data which the Counterparty processes on behalf of CWG, it must keep records of:

6.1.1 the types and categories of Protected Data and its processing activities;

6.1.2 information on overseas transfers;

6.1.3 a description of security measures implemented;

6.1.4 why and how the data is being processed;

6.1.5 the purpose of the processing;

6.1.6 any special categories of data including sensitive personal data;

6.1.7 the categories of data subjects;

6.1.8 who it shares the data with; and

6.1.9 how long it retains data for.

## 7. SECURITY MEASURES

7.1 The Counterparty must have in place measures to maintain the integrity and confidentiality of the Protected Data it processes, including but not limited to:

7.1.1 a data protection policy and data breach and incident reporting procedure;

7.1.2 adequate data encryption and pseudonymisation appropriate to the type and amount of Protected Data being processed;

7.1.3 systems' resilience to ensure the data can be restored quickly after an incident or date breach;

7.1.4 encrypted data transfer, secure storage and firewalls, intrusion detection software, access controls and reporting, anti-virus and anti-malware, data loss prevention, systems monitoring, security threat analysis and preventative security patching;

7.1.5 assessment and evaluation processes;

7.1.6 adequate access controls and asset management to protect the security of its physical environment; and processes and contractual terms to allow it to supervise its suppliers.

## 8. INDEMNITY

8.1 The Contracting Party shall indemnify CWG and keep CWG indemnified against all losses, claims, damages, liabilities, fines, interest, penalties, costs, charges, sanctions, expenses, compensation paid to Data Subjects (including compensation to protect goodwill and ex gratia payments), demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a Data Protection Supervisory Authority) arising out of or in connection with any breach by the Counterparty of its obligations relating to Protected Data under this code of practice or the Agreement.

8.2 All amounts paid or payable by CWG to a third party which would not have been paid or payable if the Counterparty's breach of its obligations relating to Protected Data under this code of practice or the Agreement had not occurred.

## 9. SURVIVAL

9.1 This code of practice shall survive termination or expiry of the Agreement for any reason.

## APPENDIX

### Data Processing and Security Details

**Section 1 - Data Processing Details**

Processing of the Protected Data by the Counterparty under the Agreement and in accordance with this code of practice shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out below or in the Agreement.

**Subject-matter of processing:**
The Subject matter of the processing of the Protected Data shall be as set out in the Agreement.

**Duration of the processing:**
Until the Processing End Date or satisfaction of the Counterparty's obligations relating to return or deletion of the Protected Data.

**Nature and purpose of the processing:**
Protected Data will be processed in support of the services provided under the Agreement and for the purposes of recording, auditing and identification purposes.

**Type of Personal Data:**
Personal Data including names, addresses, dates of birth, contact details (including phone and e-mail address) and such other personal data that may be included in correspondence and documentation arising in connection with the performance and enforcement of the Agreement and having regard to the nature of the Agreement may include:

- public and consented data relating to tenants and residents, including financial details (sort codes and account numbers)
- data held by third parties such as credit agencies payments made information.
- CCTV footage
- Audio Recordings
- Entry and exit data from sites and other areas/access points (which may include special category data for restricted areas)
- Health data relating to tenants and residents and visitors

**Categories of Data Subjects:**
Personnel involved in the performance of the Services provided under or pursuant to the Agreement.

Depending on the nature of the Agreement, other data subjects may include personal data relating to:

- Residents
- Tenants
- Visitors to the CGW estate or CWG websites
- Employees and visitors of third-party companies who undertake business on the CWG estate
- Trade Contractors' sub-contractor and supplier personnel

**Recipients of the Personal Data**

- The parties in connection with the provision of services under any Agreement.
- Personnel and their appointed or authorised representatives including debt management companies.
- The personnel of other contractors and consultants engaged in connection with an Agreement.
- Third Party suppliers of services **to** CWG where required e.g. for granting access to Site or deliveries.

**Specific processing instructions:**

Please refer to any such instructions contained in the Agreement.

**CWG DPO**

E-mail: dataprotection@canarywharf.com

**Section 2 - Minimum Technical and Organisational Security Measures**

Without prejudice to its other obligations, the Counterparty shall implement and maintain at least the following technical and organisational security measures to protect the Protected Data:

In accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with the Agreement, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, the Counterparty shall implement appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the UK GDPR.

Without prejudice to its other obligations, the Supplier shall also satisfy any relevant specific security measures set out in the Agreement.