Data Protection Procedure (GDPR Compliant) Policy

NOTE: This policy supersedes all previous Data Protection Procedure policies

1.0 Purpose

This Data Protection Procedure sets out the principles that Cleveland Bridge UK Limited ("CBUK" or "we", "us" or "our") will follow when obtaining, handling, processing, transporting or storing personal data in the course of its operations and activities including but not limited to customer, supplier and employee data.

The purpose of this Data Protection Procedure is to enable CBUK and its employees, Directors and officers to comply with all data protection laws, including but not limited to the General Data Protection Regulations ((EU) 2016/679) ("GDPR").

This procedure sets out how CBUK handle the Personal Data of our customers, suppliers, employees, workers and other third parties. This procedure applies to all Personal Data CBUK Processes regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

For the purposes of this procedure the following definitions will apply:

- Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which significantly affects an individual. Unless certain conditions are met, ADM is prohibited by GDPR.
- Automated Processing: any form of automated processing of Personal Data, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. CBUK do not carry out any Automated Processing.
- Consent: agreement which must be freely given, specific, informed and an unambiguous indication that the Data Subject agrees to the Processing of their Personal Data.
- Data Controller: the person or organisation that determines when, why and how to process Personal Data. CBUK are the Data Controller of all Personal Data relating to CBUK Personnel and Personal Data used for our own commercial purposes.
- Data Subject: a living and identifiable person about whom we hold Personal Data. Data Subjects may be nationals or residents of any country. Data Subjects may include but are not limited to past and current employees, agency staff, temporary workers, work experience staff, people from related companies, employees of our subcontractors, vendors, customers, professional advisors, clients and other third parties.
- Data Privacy Impact Assessment: shall mean a "DPIA", i.e. an assessment used to identify and reduce the risks of a data processing activity. DPIA's should be carried out in accordance with Section 9.
- EEA: All members of the European Union, Iceland, Liechtenstein and Norway.
- Explicit Consent: consent which requires a very clear and specific statement.
- Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify from that data alone or in combination with other reasonably accessible information. Personal Data includes Special Category Data and pseudonymised Personal Data but does not include anonymous data. Personal data may be factual, e.g. a name, email address, location or birth date, or an opinion about that person's actions or behaviour. Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
- Privacy Notices: separate notices setting out information that is provided to Data Subjects when CBUK collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

- Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding data, or carrying out any operation/s on data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
- Related Procedures: CBUK's policies, procedures or processes related to this procedure, including but not limited to the (i) Document Retention Procedure, (ii) Information Security and Acceptable Usage Procedure, (iii) Data Protection Impact Assessment Template & (iv) CBUK's record of processing activities.
- Special Category Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2.0 Eligibility

This procedure applies to all individuals working for or on behalf of CBUK at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, home workers, casual workers and agency staff, agents, or any other person associated with CBUK, wherever located (hereinafter "CBUK Personnel").

It is the responsibility of all CBUK Personnel to read and understand this procedure and ensure they comply with the standards and behaviours outlined herein.

Any employee who breaches this procedure will be fully investigated in line with CBUK disciplinary procedures and may face disciplinary action, which could result in dismissal for gross misconduct. Any non-employee who breaches this procedure may have their contract terminated with immediate effect.

This procedure does not form part of any employee's contract of employment and CBUK may amend it at any time.

3.0 Ownership and Responsibility

CBUK's Directors shall have ultimate responsibility for the implementation and adoption of CBUK's Data Protection Procedure. CBUK's Directors recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility of all CBUK Personnel. CBUK is exposed to potential fines of up to EUR €20 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

The Data Management Team shall have the "day to day" responsibility for managing and reviewing this procedure, however each Departmental Head and / or Department Manager shall have full responsibility for ensuring compliance with this procedure within their own departments.

4.0 Ownership and Responsibility

CBUK is responsible for and must be able to demonstrate compliance with data protection law. In order to ensure that CBUK meets its responsibilities, it is essential that CBUK Personnel comply with data protection law, this Data Protection Procedure and all Related Procedures when Processing Personal Data. We have set out below the key obligations under data protection laws and details of how CBUK expect CBUK Personnel to comply with these requirements. Personal Data must be:
(a) Processed lawfully, fairly and in a transparent manner (Section 4.1 below),

(b) Collected only for specified, explicit and legitimate purposes (Section 4.2 below),

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Section 4.3 below),

(d) Accurate and where necessary kept up to date (Section 4.4 below),

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Section 4.5 below),

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Section 4.6 below),

(g) Not transferred to another country without safeguards being in place (Section 4.7 below), &

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Section 4.8 below).

4.1 Lawfulness, Fairness and Transparency

All Personal Data must be Processed lawfully, fairly and in a transparent manner. GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but are intended to ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

CBUK must only process Personal Data on the basis of one or more of the lawful bases set out below:

(a) the Data Subject has given Consent (not available if the Data Subject is an employee), or

(b) the Processing is necessary for the performance of a contract with the Data Subject, or

(c) the Processing is necessary to meet our legal compliance obligations, or

(d) the Processing is necessary to protect the Data Subject's vital interests, or

(e) the Processing is necessary to pursue our legitimate interests which do not prejudice the interests or fundamental rights and freedoms of the Data Subjects.

Consent

Consent must be freely given, specific, informed and unambiguous. A Data Subject may consent to the Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Consent – Special Category Data

If no other lawful basis is available, CBUK must attain Explicit Consent for the Processing of Special Category Data, for Automated Decision-Making and for cross border data transfers. In these circumstances, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent. You will need to evidence Consent captured and keep records of all Consents so that CBUK can demonstrate compliance with Consent requirements.

Transparency

GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Management Team and how & why we will use, Process, disclose, protect and retain

that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

What you need to do

You must only Process Personal Data in accordance with your lawful job duties and in accordance with your departmental procedures and processes. The Data Management Team should be informed of any new Processing such as the creation of new forms to collect Personal Data, to ensure that CBUK's record of processing activities is kept up to date and this Data Protection Procedure is complied with.

4.2 Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

What you need to do

You must only use the Personal Data that you Process during your duties for CBUK's legitimate and authorised purposes. You must never Process Personal Data for any purposes unrelated to your job duties. The Data Management Team should be informed if you need to Process Personal Data for a different purpose to which it was collected.

4.3 Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

What you need to do

You must only acquire and Process Personal Data that you actually need for CBUK's legitimate purposes. You must comply with CBUK's Document Retention Policy.

4.4 Accuracy

Personal Data must be accurate, complete and relevant to the purpose for which it was collected. It must be corrected or deleted without delay when inaccurate or no longer relevant.

What you need to do

You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data as soon as possible. Personal Data should be stored centrally and must never be stored on unencrypted portable storage or your hard drive.

4.5 Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

What you need to do

You must comply with CBUK's Document Retention Procedure.

4.6 Security, Integrity and Confidentiality

CBUK will secure Personal Data by the use of appropriate technical and organisational measures to protect against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. CBUK will

regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

What you need to do

You must comply with all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction including but not limited to CBUK's Information Security and Acceptable Usage Procedure. You should comply with the confidentiality requirements (below).

Confidentiality – CBUK Personnel

You may only share the Personal Data we hold with other CBUK Personnel if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

Confidentiality – Third Parties

You may not share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with third parties, such as service providers, professional advisors and companies related to CBUK if:

(a) the category of data is included in the record of processing activities along with the third party to whom the information is to be shared with,

(b) the third party have a need to know the information for the purposes of providing the contracted services or other legitimate reason,

(c) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained

(d) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place,

(e) the transfer complies with any applicable cross border transfer restrictions, and

(f) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

If any of these requirements are outstanding, you must contact the Data Management Team.

4.7 Transfer Limitation

GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if you have express approval from the Data Management Team. This approval will only be given if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms,

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, etc.,

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims and, in some limited cases, for our legitimate interest.

What you need to do

You must ensure you have prior approval from the Data Management Team for any Personal Data transfer outside of the EEA.

4.8 Data Subject Rights and Requests

Data Subjects have certain rights in relation to their Personal Data. These include:

(a) The right to make a 'subject access request'. This entitles an individual to receive a copy of the Personal Data we hold about them, together with information about how and why we Process it and other rights which they have (as outlined below). This enables them, for example, to check we are lawfully Processing their data and to correct any inaccuracies.

(b) The right to request that we correct incomplete or inaccurate Personal Data that we hold about them.

(c) The right to withdraw any consent which they have given.

(d) The right to request that we delete or remove Personal Data that we hold about them where there is no good reason for us continuing to Process it. Individuals also have the right to ask us to delete or remove their Personal Data where they have exercised their right to object to Processing (see below).

(e) The right to object to our Processing of their Personal Data for direct marketing purposes, or where we are relying on our legitimate interest (or those of a third party), where we cannot show a compelling reason to continue the Processing.

(f) The right to request that we restrict our Processing of their Personal Data. This enables individuals to ask us to suspend the processing of Personal Data about them, for example if they want us to establish its accuracy or the reason for processing it.

(g) The right to request that we transfer to them or another party, in a structured format, their Personal Data which they have provided to us (also known as the right to 'data portability').

(h) The right to challenge a decision based solely on profiling/automated processing, to obtain human intervention, and to express their point of view.

We are required to comply with these rights without delay and in respect of certain rights within one month. Data Subjects have the right to complain to the Information Commissioners Office (ICO) and to take action in court to enforce their rights and seek compensation for damages suffered as a result of any breaches.

What you need to do

If a Data Subject invokes any of his rights (as above) you must verify the identity of the individual and immediately inform the Data Management Team of the request. You must not share any information with the Data Subject until approval is granted from the Data Management Team.

5.0 Accountability and Demonstrable Compliance

CBUK are responsible for and must be able to demonstrate compliance with the data protection principles listed in Section 4.

CBUK, through the Data Management Team must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Management Team is responsible for, and must be able to demonstrate, compliance with the data protection principles. Compliance will be demonstrated through the following:
(a) Appointment of a Data Management Team consisting of suitably qualified senior managers.
(b) Ensuring DPIAs are completed where Processing represents a high risk to the rights and freedoms of Data Subjects.
(c) Maintaining, reviewing and updating this procedure and all Related Procedures.
(d) regularly train CBUK Personnel on GDPR, this procedure and Related Procedures, and

(e) the Data Management Team led by the Compliance Manager will monitor the effectiveness and review the implementation of this Procedure. The review shall take place on a 6-monthly basis.

6.0 Data Management Team

The Data Management Team have responsibility for data protection compliance. The team consists of:

i) Compliance Manager (chair)
ii) IT Manager
iii) Head of SHE
iv) Finance Representative
v) HR Representative

The Data Management team shall meet on a 6-monthly basis to review this procedure and any Related Procedures. In addition, the Data Management team may meet if required to do so under the GDPR Procedure or due to a reason arising under this procedure.

This list is an example of areas where the Data Management Team should be involved. In each case it is your responsibility to ensure you have first taken the matter to your departmental manager who may be able to provide assistance.

(a) There has been a Personal Data Breach (follow the process in Section 12),

(b) You have received a data subject access request,

(c) You are unsure of the lawful basis which you are relying on to process Personal Data,

(d) You need to rely on Consent and/or need to capture Explicit Consent,

(e) You need to draft Privacy Notices,

(f) You are unsure about the retention period for the Personal Data being Processed,

(g) You are unsure about what security or other measures you need to implement to protect Personal Data,

(h) You are unsure on what basis to transfer Personal Data outside the EEA,

(i) You are engaging in a significant new, or change in, Processing activity which may require a DPIA or you plan to use Personal Data for purposes others than what it was collected for,

(j) You plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making,

(k) You need help complying with applicable law when carrying out direct marketing activities,

(l) You are unsure whether Processing being carried out is captured on CBUK's record of data processing activities,

(m) You need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

7.0 Record of CBUK's Data Processing Activities

Th GDPR requires CBUK to keep a full and accurate record of all our data Processing activities. It is the responsibility of all departmental managers to ensure that any Processing of Personal Data that is carried out within your departments or on your behalf by other departments or third parties is included in CBUK's record of data processing activities.

If in doubt, contact the Data Management Team for confirmation. The record of data processing activities will include, as a minimum; (i) clear descriptions of the Personal Data types, (ii) Data Subject types, (iii) Processing activities, (iv) Processing purposes, (v) third-party recipients of the Personal Data, (vi) Personal

Data storage locations, (vii) Personal Data transfers, (viii) the Personal Data's retention period, and (ix) a description of the security measures in place.

8.0 Privacy Notices

Privacy Notices must be approved by the Data Management Team prior to issue.

9.0 Data Privacy Impact Assessments (DPIA)

CBUK must conduct DPIA's in respect to high risk Processing. The DPIA must be completed prior to implementing any major system or business change programs involving the Processing of Personal Data including (but not limited to):

(a) the use of new technologies (programs, systems or processes), or changing technologies,

(b) the use or change of use of CCTV technology,

(c) any Automated Processing including profiling and Automated Decision Making, and

(d) large scale Processing of Special Category Data.

The DPIA should include:

(a) a description of the Processing, its purposes and CBUK's legitimate interests if appropriate,

(b) an assessment of the necessity / proportionality of the Processing in relation to its purpose,

(c) an assessment of the risk to Data Subjects, and

(d) the risk mitigation measures in place and demonstration of compliance.

If a DPIA is required, you must contact the Data Management Team.

10.0 Automated Processing (including profiling) and Automated Decision Making

CBUK do not currently carry out any Automated Processing (including profiling) or Automated Decision Making. The Departmental Manager is to contact the Data Management Team if Automated Processing or Automated Decision Making is proposed.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

11.0 Direct Marketing

Consent for direct marketing ("opt-in"):

A Data Subject's prior consent is required for any direct marketing. In order to be valid, Consent must be specific and informed. As such, CBUK should provide the following information as a minimum:

(a) the name of your organisation and the names of any third parties who will rely on the consent,

(b) the purposes of the processing,

(c) the processing activities, and

(d) how to withdraw consent for processing.

Soft opt-in:

The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first

collecting the details and in every subsequent message. This allows direct marketing to existing contacts but does not include other communications.

Objection to direct marketing ("opt-out"):

All direct marketing must have a mechanism allowing the recipient to "opt-out" of future marketing. This mechanism must be as straightforward as possible, and CBUK must ensure that the opt-out request is complied with as soon as possible. If a customer opts out their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future, this may include removing all references to the Data Subject from our systems.

12.0 Reporting a Personal Data Breach

Personal Data Breaches may include (but isn't limited to) lost or mislaid equipment or data, use of inaccurate or excessive data, failure to address an individual's rights, accidently sending data to the wrong person, unauthorised access to, use of or disclosure of data, deliberate attacks on CBUK's IT systems or thefts of records and any equivalent breaches by CBUK's third party providers.

Where there has been a Personal Data Breach CBUK must take immediate action to contain the risks, remedy the breach and notifying the Information Commissioners Office (ICO) and the Data Subject where legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the IT Department by telephone to report the breach. If the breach has occurred outside of normal business hours, you must leave a voice message detailing your name and contact details, outlining the data breach and when the breach occurred. You should also ensure you inform your line manager.

Contact number for reporting breaches: 07900 678464

Once you have reported the breach to the ICT Department, you must send an email outlining the details of the breach to the following individuals:

Email address for reporting breaches: data-protection@clevelandbridge.com

13.0 Training/Education

All office-based employees should be properly trained on data protection. All personnel in "high-risk" departments, i.e. departments identified as having a higher likelihood of processing Personal Data such as Human Resources, Training, Finance, SHE and Payroll will undertake specific GDPR training. This procedure is to be given to all office based or site-based staff members as part of the employee induction process.

It is the responsibility of all Departmental Managers to review all the systems and processes under your control to ensure they comply with this procedure and check that adequate controls and resources are in place to ensure proper use and protection of Personal Data.

All office-based employees must sign a confirmation statement acknowledging that they have attended Data Protection training (this may be as part of the employee induction process) and that they understand the Data Protection Procedure's requirements.

14.0 Questions and Concerns

Any questions about this procedure should be referred to the Compliance Manager. If the Compliance Manager is unavailable, questions may be forwarded to any other member of the Data Management Team.