Data Protection Policy & Procedures

Contents

1 POLICY STATEMENT

Carter Ceilings Limited *(hereinafter referred to as the **"Company"**)* needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)***, ***UK data protection laws*** and any other relevant the data protection laws and codes of conduct *(herein collectively referred to as **"the data protection laws"**).*

The Company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a ***'Privacy by Design'*** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2 PURPOSE

The purpose of this policy is to ensure that the Company meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

The data protection laws include provisions that promote accountability and governance and as such the Company has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

3 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.1 DEFINITIONS

- ***"Biometric data"*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- ***"Binding Corporate Rules"*** means personal data protection policies which are adhered to by the Company for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
- ***"Consent"*** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- ***"Data controller"*** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- ***"Data processor"*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- ***"Data protection laws"*** means for the purposes of this document, the collective description of the GDPR, Data Protection Act 2018 (*referred to as the Act*) and any other relevant data protection laws that the Company complies with.
- ***"Data subject"*** means an individual who is the subject of personal data
- ***"GDPR"*** means the *General Data Protection Regulation (EU) (2016/679)*
- ***"Genetic data"*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- ***"Personal data"*** means any information relating to an identified or identifiable natural person *('data subject'*); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- ***"Processing"*** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- ***"Profiling"*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- ***"Recipient"*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- ***"Supervisory Authority"*** means an independent public authority which is established by a Member State
- ***"Third Party"*** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

4 DATA PROTECTION BACKGROUND

The UK initially had The Data Protection Act 1984 in place to regulate the use of processed information that related to individuals. However, in 1995 the introduction of EU Directive 95/46/EC which set aims and requirements for member states on the protection of personal data when processing or sharing, meant an updated Act was required.

The UK subsequently developed and enacted The Data Protection Act 1998 (DPA) to ensure that British law complied with the EU Directive and to provide those with obligations under the Act, with updated rules, requirements and guidelines for processing and sharing personal data.

2018 marks the 20th anniversary of the DPA enactment and whilst there have been periodical additions or alterations to the Act, technology has advanced at a far faster rate, necessitating new regulations for the current digital age. The past 20 years has also seen a vast increase in the number of businesses and services operating across borders, further highlighting the international inconsistency in Member States data protection laws.

For this reason, in January 2012, the European Commission proposed a new regulation applying to all EU Member States and bringing a standardised and consistent approach to the processing and sharing of personal information across the EU.

4.1 NATIONAL DATA PROTECTION LAW

As the Company is in the UK, we are obligated under the GDPR and the UK's Data Protection Act 2018 that implements the GDPR into UK law. Our data protection policies and procedures adhere to both the GDPR and Data Protection Act 2018 requirements, as applicable to our business type.

4.2 GENERAL DATA PROTECTION REGULATION (GDPR)

The ***General Data Protection Regulation (GDPR) (EU)2016/679)*** was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the Company processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

4.2.1 PERSONAL DATA

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The Company ensures that a high level of care is afforded to personal data falling within the GDPR's **'special categories'** *(previously **sensitive personal data***), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that: -

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies."

4.2.2 THE GDPR PRINCIPLES

Article 5 of the GDPR requires that personal data shall be: -

- processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')*** and requires that firms ***show how*** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

4.3 THE INFORMATION COMMISSIONERS OFFICE (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Act 2018 (GDPR)
- Data Protection, Privacy and Electronic Communication (amendments etc EU exit) Regulations 2019
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

The ICO's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in the UK.

The Company are registered with ICO and appear on the Data Protection Register as a data controller of personal information.

Our Data Protection Registration Number is ZB535616.

4.4 DATA PROTECTION OFFICER

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by a firm where: -

- The processing is carried out by a public authority or body *(except for courts acting in their judicial capacity)*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

Where the Company has appointed a designated data protection officer, we have done so in accordance with the GDPR requirements and have ensured that the assigned person has an adequate and expert knowledge of data protection law. They have been assessed as being fully capable of assisting the Company in monitoring our internal compliance with the Regulation and supporting and advising employees and associated third parties with regards to the data protection laws and requirements.

The data protection officer for Carter Ceilings is Alison Warrender.

5 OBJECTIVES

We are committed to ensuring that all personal data processed by the Company is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Company has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The Company ensures that: -

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where we have verified and met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements and in compliance with the Data Protection Act 2018 Schedule 1 conditions
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their specific role and the Company

- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed a Data Protection Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We conduct internal audits which includes how the personal data we process is obtained, used, stored and shared, and includes policies, procedures and the relevant legal and other requirements.
- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy all personal information, in accordance with our register of records (CCR04) which has been developed from the legal, regulatory and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws through communication of this policy (CCP05)
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements
- We maintain compliance with Document Control (CCSP01) and Records (CCSP02). We have a robust information security system in place which is management by our externally contracted I.T. company.

6 ACCOUNTABILITY & COMPLIANCE

Our main objectives are to: -

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance. This includes induction and refresher training
- Identify key stakeholders and allocate responsibility for data protection compliance, and ensure that the designated person(s) has sufficient access, support and budget to perform the role

The technical and organisational measures that the Company has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

6.1.1 PRIVACY BY DESIGN

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures *(detailed below*), that help us enforce this ethos.

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection *(i.e. forms, website, surveys etc*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include *'optional'* fields, as optional denotes that it is not necessary to obtain
- Physical collection *(i.e. face-to-face, telephone etc*) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- Where required we will comply with destruction procedures where a data subject or third party provides us with personal information that is surplus to requirements.
- Personal data held by Carter Ceilings is reviewed under the audit schedule, to ensure that they are fit for purpose and comply with this policy.

Our *Privacy by Design* approach means that personal data is protected through restricted access. Refer to our system procedure Document Control (CCSP01) and Records, CCSP02

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for. ***Steps include: -***

- In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject
- Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (*i.e. when the data is being passed to a third-party for processing and not directly to the data subject*)
- When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (*i.e. we do not use the postal system as this can be intercepted*).
- Recipients (*i.e. the data subject, third-party processer*) are reverified and their identity and contact details checked
- The Data Protection Officer authorises the transfer and checks the file(s) attached and encryption method and key
- Once confirmation has been obtained that the recipient has received the personal information, where possible *(within the legal guidelines and rules of the data protection laws*), we destroy the hard copy data and delete the sent message
- If for any reason a copy of the paper data must be retained by the Company, we use a physical safe to store such documents as oppose to our standard archiving system

INFORMATION AUDIT

To enable the Company to fully prepare for and comply with the data protection laws, we have carried out a company-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our company in our capacity as a controller/processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
-

7 Legal Basis for Processing *(Lawfulness*)

At the core of all personal information processing activities undertaken by the Company, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information audit register and in our Privacy Notice and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. ***Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -***

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).*

6.1.1 PROCESSING SPECIAL CATEGORY DATA

Special categories of Personal Data are defined in the data protection laws as: -

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the Company processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR regulations and in compliance with the Data Protection Act 2018 Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We will only ever process special category data where: -

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Schedule 1, Parts 1, 2 & 3 of The Data Protection Act 2018 provide specific conditions and circumstances when special category personal data can be processed and details the requirements that organisations are obligated to meet when processing such data.

Where the Company processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing. ***Measures include: -***

- Verifying our reliance on one of the data protection laws Article 9(1), and where applicable The Data Protection Act 2018 Sch.1, Pt.1, Pt.2 and/or Pt.3 conditions prior to processing
- Documenting the Schedule 1 condition and Article 6(1) legal basis relied upon from processing on our Processing Activities Register (*where applicable)*
- Having an appropriate policy document in place when the processing is carried out, specifying our: -
    - procedures for securing compliance with the data protection laws principles
    - policies as regards the retention and erasure of personal data processed in reliance on the condition
    - retention periods and reason *(i.e. legal, statutory etc)*
    - procedures for reviewing and updating our policies in this area

Please refer to our document Control (CCSP01) and Records CCSP02) for guidance..

6.1.2 RECORDS OF PROCESSING ACTIVITIES

As an organisation with ***less than*** 250 employees, the Company does not maintain records of our processing activities. However, we continually review all such activities and company size to ensure that we will record such information as detailed in GDPR Article 30 where: -

- We employee 250 or more employees
- Processing personal data could result in a risk to the rights and freedoms of individual
- The processing is not occasional
- We process special categories of data or criminal convictions and offences

- Such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Supervisory Authority upon request.

Acting in the capacity as a processor (*or a representative*), our internal records of the categories of processing activities carried out on behalf of a controller, contain the following information: -

- The full name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer
- The categories of processing carried out on behalf of each controller
- A general description of the processing security measures as outlined in section 13 of this document *(pursuant to Article 32(1) of the data protection laws)*

Third-Party Processors

The Company utilise external processors for certain processing activities *(where applicable*). We use information audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. ***Such external processing includes*** *(but is not limited to****): -***

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources
- Hosting or Email Servers
- Credit Reference Agencies

We have strict due diligence and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

We draft bespoke Service Level Agreements (SLAs) and contracts with each processor as per the services provided and have a dedicated Processor Agreement template that details: -

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

The Processor Agreement and any associated contract reflects the fact that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (*unless required to do so by a law to which the processor is subject*)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the Company in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to the Company after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the Company all information necessary to demonstrate compliance with the obligations set out in the agreement and contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs the Company immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

Data Retention & Disposal

The Company have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritises the protection of the personal data in all instances.

Please refer to our System Proceedure, Records (CCSP02) for full details on our retention, storage, periods and destruction processes.

7 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The Company does not currently carry out any processing activities that are defined as requiring a DPIA, however we monitor all activities against the GDPR Article 35 requirements Data Subject Rights Procedures.

7.1 CONSENT & THE RIGHT TO BE INFORMED

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by the Company and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

The data protection law defines consent as; *'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.*

Where processing is based on consent, the Company have reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes

- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand
- Pre-ticked, opt-in boxes are **never** used
- Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is **not** be a precondition of any service (*unless necessary for that service)*
- Along with our company name, we also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our company name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
    - Opt-out links in mailings or electronic communications
    - Opt-out process explanation and steps on website and in all written communications
    - Ability to opt-out verbally, in writing or by email
- Consent withdrawal requests are processed immediately and without detriment
- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified

7.1.1 CONSENT CONTROLS

The Company maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Data Protection Officer prior to being circulated.

Consent to obtain and process personal data is obtained by the Company through: -

- Face-to-Face
- Telephone
- In Writing
- Email/SMS
- Electronic *(i.e. via website form*)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, granular and utilises a demonstrable opt-in mechanism. Where consent is obtained verbally, we utilise scripts, checklists to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Electronic consent is always by a non-ticked, opt-in action (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS or written confirmation of the consent to process, store and share the personal information.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

7.1.2 ALTERNATIVES TO CONSENT

The Company recognise that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent but would still process it even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use
- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate
- Where there is an imbalance in the relationship, i.e. with employees

7.1.3 INFORMATION PROVISIONS

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*)), we provide the below information in all instances, **in the form of a privacy notice: -**

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party",* details of the legitimate interests
- The recipients or categories of recipients of the personal data *(if applicable)*
- If applicable, the fact that the Company intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
    - where the Company intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards the Company has put into place and the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability

- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

7.2 COMMUNICATION

This policy provides the legal information on how we handle, process and disclose personal information. Carter Ceilings communicate the policy at induction, via our website, refresher updates and on request. A simplified version is contained in the company handbook.

The data protection officer is responsible for reviewing, maintaining and communication the data protection policy. Feedback on the contents of this policy and how to improve effectiveness of this policy is welcomed.

Where we rely on consent to obtain and process personal information, we ensure that it is: -

- Displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing

7.3 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

Where the Company obtains and/or processes personal data that has **not** been obtained directly from the data subject, the Company ensures that the information disclosures contain in Article 14 are provided to the data subject within 30 days of our obtaining the personal data *(except for advising if the personal data is a statutory or contractual requirement).*

In addition to the information disclosures in section 8.1.4, where personal data has not been obtained directly from a data subject, we also provide them with information about: -

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure.

Where the Company intends to further process any personal data for a purpose ***other*** than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in the relevant section of this policy, we reserve the right not to provide the data subject with the information if: -

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by Union or Member State law to which the Company is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

7.3.1 EMPLOYEE PERSONAL DATA

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. We ensure at induction that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Employee Handbook (CCF19) which informs them of their rights under the data protection laws and how to exercise these rights and are provided with this policy (CCP05) specific to the personal information we collect and process about them.

7.4 THE RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

7.4.1 SUBJECT ACCESS REQUEST

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period

- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the Company from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the Data Protection Officer as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Please refer to our Employee Handbook and the data protection officer for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the data protection laws.

7.5 DATA PORTABILITY

The Company provides all personal information pertaining to the data subject to them on request and in a format, that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the data protection laws concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from the Company to a designated controller, where technically feasible.

We utilise the below formats for the machine-readable data: -

- HTML
- CSV
- XML
- RDF
- XHTML

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

7.6 RECTIFICATION & ERASURE

7.6.1 CORRECTING INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d), all data held and processed by the Company is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The Data Protection Officer are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

7.6.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be Forgotten'*, the Company complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the Company is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

Please refer to our Register of Records for exact procedures on erasing data and complying with the Article 17 requirements.

7.7 THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where the Company restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The Company will apply restrictions to data processing in the following circumstances: -

- Where an individual contest the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (*where it was necessary for the performance of a public interest task or purpose of legitimate interests*), and we are considering whether we have legitimate grounds to override those of the individual

- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Data Protection Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

7.8 OBJECTIONS AND AUTOMATED DECISION MAKING

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information.

Individuals have the right to object to: -

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling*)
- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where the Company processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on *'grounds relating to their particular situation'*. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where a data subject objects to data processing on valid grounds, the Company will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention. We also assess new systems and technologies for this same component prior to implementation. the Company understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the data protection laws, we aim to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: -

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual

In limited circumstances, the Company will use automated decision-making processes within the guidelines of the regulations. ***Such instances include: -***

- Where it is necessary for entering into or performance of a contract between us and the individual
- Where it is authorised by law *(e.g. fraud or tax evasion prevention)*

- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where the Company uses, automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

8 OVERSIGHT PROCEDURES

8.1 SECURITY & BREACH MANAGEMENT

Alongside our *'Privacy be Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Refer to Document Control (SP01) and Records (SP02)

We carry out internal audits to ensures that our management system adequately addresses information security risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, in the event of this occurring Carter Ceilings will comply with the ICO guidance. 72 hours - how to respond to a personal data breach | ICO

9.0TRANSFERS & DATA SHARING

Carter Ceilings do not share personal data to companies outside the UK.

Where data is being transferred for a legal and necessary purpose, Carter Ceilings will ensure protection either by encryption and/or password..

9 AUDITS & MONITORING

Carter Ceilings conduct internal audits to ensure the management system is suitable, adequate and effective. The Data Protection Officer has overall responsibility for ensuring this policy is effective implemented.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

10 TRAINING

Training and awareness on data protection requirements delivered at induction and bespoke mentoring depending on the role. A copy of policies and procedure are available upon request.

11 PENALTIES

The Company understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. ***We recognise that: -***

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to £8.7million or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to £17.5million or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

12 RESPONSIBILITIES

The Company has appointed a Data Protection Officer whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up to date with all legislation and changes relating to data protection.

The DPO will work with others to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with data protection training and will be subject to development support and mentoring to ensure that they are competent and knowledgeable for the role they undertake.

This Policy has been approved and authorised by:

Name: **Niall J.M. Miller**

Position: **Managing Director**

Date: **June 2023**

Signature: