DATA PROTECTION

2021

,

C&R CAPITAL & REGIONAL

DATA PROTECTION

This policy sets out how Capital & Regional, Mall People and its staff must collect, store and process personal data in order to comply with the EU General Data Protection Regulations (GDPR). It sets out our legal requirements and is applicable to all staff. Compliance to this policy is a requirement of employment with Capital & Regional and its subsidiary companies.

This policy covers all Capital & Regional and Mall People staff, either permanently or temporarily employed.

Staff shall be accountable for their actions and anyone willfully, knowingly or negligently breaching the policy may be subject to disciplinary action, up to and including termination of the employment and / or legal action in instances where actions do not comply with the EU General Data Protection Regulations or subsequently introduced equivalent UK regulations.

IMPORTANT TERMS

GDPR	General Data Protection Regulations
Data Controller	A person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. For the purposes of this policy Capital & Regional is the Data Controller.
Data Processor	Data processor, in relation to personal data, means any person (other than an employee of the data controller) or organisation who processes the data on behalf of the data controller.
Information Commissioners Office (ICO)	The ICO is the UK regulatory body in charge of issues relating to Data Protection. The ICO issues guidance on the EU General Data Protection Regulations and states how it will apply under UK law. It has the power to audit organisations on issues relating to data protection and is the body that issues fines for breeches and non-compliance (up to 4% of global turnover).

Personal Data is defined as any data which can be used to identify an individual. It includes but is not limited to: names, addresses, email addresses, telephone numbers, postal addresses, device identifying information (such as IP or MAC addresses). If you are in doubt as to whether a particular item is classified as personal data please contact your line manager.

Capital & Regional, Mall People and its staff will abide by the following guiding principles in relation to the collection, storage and processing of personal data:

Personal data will be processed lawfully, fairly and in a transparent manner in relation to individuals. Personal data will be 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 not be considered to be incompatible with the initial purposes;

Personal data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Personal data will be 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.

Data will be 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

Information will be 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.

DATA SUBJECT'S RIGHTS

Capital & Regional and its staff will uphold data subject's rights as specified in the GDPR, namely:

- The right to be informed: This means individuals have the right to know how and why their data is being collected or processed.
- The right of access: individuals have a right to access the data we hold on them.
- The right to rectification: subjects must be able to fix or notify us of errors in the data
- The right to erasure: Data subjects are able to request the secure deletion of their data.
- The right to restrict processing: Individuals have the right to restrict how their data is processed and used.
- The right to data portability: Subjects must be able to move their data to other systems and the format of data must enable such transfers.
- The right to object: Individuals have the right to object to how their data is being used.
- Rights in relation to automated decision making and profiling.

ACCESS & DELETION REQUESTS

Individuals have the right under GDPR to request access to, modify and delete the personal data we hold about them. We will uphold these requests unless contradicted by overriding legal regulations or requirements such as accident reports required for health & safety purposes. Requests must be processed with 30 days and at no cost to the data subject.

Access and deletion requests for guest data should be passed to the Marketing line manager within 7 days of being received.

TRANSPORTATION OF DATA

Personal data must not be transferred by physical means, for example on laptops or USB data sticks, unless securely encrypted, with passwords transferred separately.

Passwords must be transferred separately from the data and where possible via a different method, for example issued by phone.

Passwords must be 'strong', avoiding obvious or common phrases and words. For advice on creating strong passwords please contact the IT department.

Standard email is not a secure method for the transferring of personal data and should not be considered private. It should only be used by Capital & Regional and Mall People staff in their communications internally, with clients or third parties for the transmission of routine messages and not personal data unless additional protection such as encryption is applied.

Personal data is only permitted to be downloaded from the internet where the host websites operate valid security, namely the implementation of security certificates, and access to data is password protected. Sites that operate with security certificates will be prefixed with https rather than http, and internet browser will display a padlock symbol next to the website address. If in doubt staff should contact the IT department for clarification.

Personal data must not be accessed or downloaded via public or unsecure WiFi networks.

REPORTING OF DATA BREACHES AND LOSS OF DATA

A data breaches is a security incident that has affected the confidentiality, integrity or availability of personal data and can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

It is a legal requirement for the business to report data breaches or loss of personal data that might result in a risk to people's rights and freedoms within 72 hours to the Information Commissioners Office (ICO), the UK supervisory authority.

Your line manager and the Support Office marketing team must be informed with 8 hours from the point you became aware of the possibility of a breach, who will take action to inform the ICO if required. All reasonable steps must be taken to attempt to contact your line manager. If they cannot be reached it should be escalated to the following persons:

- HR at carterhr@capreg.com
- Sara Jennings – Director of Guest & Customer Experience at sara.jennings@capreg.com

When reporting a breach, you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

RESPONSIBILITIES

Everyone within Capital & Regional and Mall People has a responsibility to ensure they collect, store and process personal data in a way in which complies to GDPR.

Board-level responsibility for compliance with GDPR lies with the Senior Leadership Team.
Centre General Managers have overall responsibility to ensure centre staff, including marketing managers understand and comply with this policy as well as the wider GDPR regulations.

DATA PROCESSORS AND THIRD-PARTY SUPPLIERS

The usage of third party companies or suppliers, referred to as Data Processors, to handle personal data on the Company's behalf requires that a written contract be in place to ensure processing carried out by a processor meets all the requirements of the GDPR. Similarly, if a processor employs another processor it needs to have a written contract in place. No employees are permitted to appoint companies to work with personal data on our behalf without an approved written contract in place.

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller (Capital & Regional).

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state

Staff involved in the appointment or management of Data Processors must be aware of Processors obligations under GDPR.

In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities;
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

If a processor fails to meet any of these obligations or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

PRIVACY IMPACT ASSESSMENTS (PIAS)

We conduct Privacy Impact Assessments (PIAs) for data processing activities considered high-risk under GDPR and when commissioning new and major systems to collect, store or hold personal data. Any staff involved in the commissioning of such systems must complete a Privacy Impact Assessment and have this approved by the support office marketing team.

PIAs must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Any identified high risks must be consulted on with the ICO before starting the processing of the data.

ACCOUNTABILITY

Article 5(2) of the GDPR requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."
This means that any staff involved in the capture and processing of personal data must record the nature of that data and detail the decisions taken regarding how that data is processed. This is an ongoing and continuous process.

MARKETING CONSENT

Using personal data for marketing communications purposes will only be carried out with valid consent or another applicable legal basis. Consent is defined under GDPR 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"

Valid consent when sought by the Company must:

- Be freely given;
- Be unambiguous;
- Be obvious and require a positive action to opt in;
- Cover the purposes of the processing and the types of processing activity;
- Specifically cover the controller's name, the purposes of the processing and the types of processing activity;
- Be unbundled from other terms and conditions;
- Be specific for the activity for which it will be used;
- Make it easy for people to withdraw consent;
- Not make use of pre-checked boxes, opt-out boxes or other default settings

The method and wording for consent must be recorded for audit and accountability purposes. Details of how to record consent are available from the Support Office marketing team.

FURTHER INFORMATION

Further information on GDPR can be obtained from the Information Commissioners Office (https://ico.org.uk)

EMPLOYEE PRIVACY STATEMENT

This Privacy Notice sets out details about the personal data that we, Capital and Regional plc, Capital and Regional Property Management Limited, and Mall People Limited ("the Company"), may collect and process about you, our employees and workers.

This Privacy Notice is non-contractual, regularly reviewed and may be amended by us from time to time.

The type of data we hold on you

The type of data that we may hold on you is set out in the Appendix attached.

Personal data is often collected directly from you, however, there may be occasions where this is supplied by a third party as detailed in the Appendix.

The purpose of processing data and legal basis

Your personal data may be processed for the following purposes:

- For recruitment and promotion purposes and to ensure you are legally able to work for us
- To give effect to the contractual relationship between you and the organisation
- To comply with legal obligations arising out of our employment/working relationship
- To make decisions about your working relationship with the organisation
- To ensure compliance with our policies and procedures such as IT and communications
- To allow for your development in terms of your role with the organisation
- To keep accurate records of your employment/engagement, including employees' disciplinaries, grievances, absences, appraisals and performance matters
- To seek professional advice and to defend claims and potential claims

We only process personal data if we have a legal basis to do so. The legal bases that we rely upon are as follows:

- Where it is necessary to perform the contract, we have entered into with you. For example, to pay you in accordance with your contract and administer benefits you are entitled to;
- Where it is necessary to comply with a legal obligation. For example, we are required to check your entitlement to work in the UK, to deduct tax, to comply with health and safety laws, to make reasonable adjustments for disabled employees and to comply with laws on working time;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests (see below);
- Where you have consented to the processing.
- The legitimate interests that we refer to above are:
- Pre-employment/engagement: Ensuring that you are qualified and suitable for the role you are applying for and not exposing us to risk by ensuring recruitment would not contravene the law (right to work etc).
- During employment/engagement:Ensuring we maintain and have access to a record of your employment/work and are able to effectively manage our working relationship with you, administer the contract we have entered into and comply with our legal/regulatory obligations during your employment/engagement.
- During and after employment/engagement: Ensuring we are able to provide references for current/former employees and ensuring we have a record of your employment/engagement with us for the defence of legal claims.

Some special categories of personal data, such as health information, is processed to carry out employment law obligations, like the duty to make reasonable adjustments for disabled employees and for health and safety purposes.

We may process data relating to special category data such as race and sex for the purpose of equal opportunities monitoring. The provision of this is entirely voluntary and the data used for these purposes is anonymised.

Where we rely on consent to process your personal data, you have a right to withdraw your consent at any time. This will not affect the lawfulness of processing based on consent before its withdrawal.

If we intend to further process your personal data for a purpose other than that for which it was collected, we shall provide you with information on this other purpose and all other information as set out in this notice.

SHARING DATA

Your data may be shared internally with the manager and/or supervisor responsible for you, and their subordinates, other managers and support staff, our HR, IT and finance functions, and external consultants engaged by us but only, in each case, to the extent necessary to allow them to carry out their duties and roles or, where appropriate, in line with business needs ("Relevant Persons").

We will share your personal information with third parties where required by law (for example with HMRC for tax purposes or where some or all of our Company is being sold), where it is necessary to administer the working relationship with you (for example information may be shared with pension providers or insurance scheme providers where you have opted for these benefits) or where we have a legitimate interest in doing so (and your interests and fundamental rights do not override those interests), for example, to seek professional advice.
Where we have no legal obligation to share your data we will ensure that the recipient of the information is bound by confidentiality obligations.
We will not share your data with any country outside the European Economic Area, save for the case of employees participating in the Company's share option schemes (see below).

In the case of employees participating in the Company's share option schemes: your data may be transferred to Guernsey for administration of the share option scheme. Data is transferred on the basis of the European Commission having issued a decision confirming that Guernsey ensures an adequate level of protection for data subjects' rights and freedoms.

RETENTION PERIODS

We will hold your personal data for the duration of your employment and not for longer than is necessary.
When deciding how long to hold your data we have regard to the purposes for which this is processed, legal and regulatory requirements (including any contractually agreed periods) and statutory limitation periods (under which it is prudent for us to retain records for longer periods).

YOUR RIGHTS

You have a number of rights in relation to the personal information that we process about you. You:

- Have the right to be informed about your data (as set out in this Privacy Notice)
- Can request access to your personal data
- Can request that your personal data be rectified if it is inaccurate or incomplete
- Can request that the processing of your personal data be restricted or erased in certain circumstances, for example, where the data is no longer necessary to meet its purpose
- Can object to processing in certain circumstances, for example where this is based on legitimate interests.
- Can receive personal data that you have provided in a structured, commonly used and machine-readable format and can have this transmitted without hindrance where the data is processed on the basis of consent or performance of a contract
- Can lodge a complaint with the Information Commissioner's Office.

If you wish to exercise any of these rights please contact HR by emailing carterhr@capreg.com.

AUTOMATED DECISION MAKING ("ADM")

ADM occurs when decisions are made about you by a computer or some other information analysing machine. Examples of this include the machine scanning of CVs, computer processed aptitude or personality tests and website profiling.

We do not use ADM.

CONTACT DETAILS

Capital & Regional plc is the data controllers and can be contacted at 22 Chapter Street London SW1P 4NP. Human Resources are responsible for assisting in the first instance with employee data protection compliance. They can be contacted by email: carterhr@capreg.com

DATA BREACHES AND LOSS OF INFORMATION – NOTIFICATION FORM

In the event of a data breach or loss, or a suspected data breach or loss, please complete the table below and submit this form as set out below.

Please see the Company's GDPR Policy for further information regarding data breaches and losses, which includes examples of data breaches and losses.

Note that there are legal requirements for the business to report certain data breaches or losses of personal data within 72 hours to the Information Commissioners Office (ICO), hence your prompt notification is required.

Your line manager and the Support Office Marketing Team or HR (contact details below) must be informed within 8 hours from the point you became aware of the breach/loss or possibility of the breach/loss. All reasonable steps must be taken to attempt to contact your line manager. If they cannot be reached, the matter should be escalated to the following persons:

Jenny Prince: Support Office Marketing Team: 020 7932 8854 / 020 7932 8132 / Dataofficer@capreg.com
Sara Jennings: Director of Guest & Customer Experience: 020 7932 8094 / 07768 555583 / Dataofficer@capreg.com
HR at carterhr@capreg.com

Information required:	**Complete below:**
Name of person reporting the data breach/loss	
Location of person reporting the data breach/loss	
Date of the data breach/loss	
Description of data breach/loss, including the following information: a description of the nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned; a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects	
Date of submission of this notification	

EMPLOYEE PRIVACY NOTICE - THE TYPE OF DATA WE PROCESS ON YOU

Recruitment Stage:

Personal contact details including name, address and email;

Information collected during the recruitment process such as your CV/application (including details of previous work experience, education and references) and answers to any interview/recruitment questions relevant to the role you applied for;

Equal opportunities information. This is not mandatory and is not made available to anyone outside of the recruitment team and their subordinates (including hiring managers and HR) save in an anonymised format so as not to identify you;

Recruitment Agencies – we may collect your personal details, details of your application and details of your experience and qualifications from the recruitment agency you applied via.

With the exception of the equal opportunities information, this information is necessary for us to enter into a contract with you and a failure to provide this may mean that we are unable to process your application and, if appropriate, offer you employment/engagement. The equal opportunities form is not mandatory and there are no consequences if you fail to provide this.

Pre-employment/engagement checks:

Proof of your identity (such as driving licence) and any relevant right to work checks;

Proof of your qualifications – you may be asked to attend our office with original documents, we will take copies;

Depending on your role, you may be asked to complete an application for a Basic Criminal Record check via the Disclosure and Barring Service ("DBS") which will verify your declaration of unspent convictions. We will then get details of your criminal convictions from the DBS;

We will contact your referees (with express consent), using the details you provide in your application, directly to obtain references, and we will process the information provided by your referees;
The above is usually part of a conditional offer of employment/engagement and therefore failure to provide these may result in us being unable to offer you employment/work. Right to work checks and the DBS checks (where required) are statutory requirements. A failure to provide this may result in us being unable to offer you employment/work.

During employment/engagement

We will ask you to provide details of your emergency contact so that we know who you would like us to contact in an emergency for you;
We will ask you to provide details of your bank account for payment purposes;
We may ask you to provide further payroll and tax information and this may also be collected from the HMRC;

We will process details of your salary and benefits information including any changes to these;
We will process details of your annual leave entitlements and annual leave you have taken, and other periods of leave taken or absence;

We process CCTV footage or images and other information obtained electronically such as swipe cards, time cards etc for the following purposes:

Detecting and observing intruders
Granting access to restricted areas
Tracking visitors who may pose a security threat
Reducing pilferage, delinquent behaviour and sabotage
Countering fraud and the misuse of corporate resources
Dealing with suspected harassment

Investigating misconduct and providing evidence for internal investigations and tribunals/courts if required.

We will process details of your working arrangements such as location, hours and working time;

We will process records of your attendance including sickness absence records;

We will process performance records including performance reviews and improvement plans;

We will process details of grievances and disciplinaries relating to you;

We will process records of applications you make for other positions within the organisation and promotions;

We will process records of any training and courses that you attend, which will be kept as part of your employment record;

We will process general employment records and HR files for you;

We will process correspondence to and from you, your opinions and information from colleagues and other third parties related to you or your work (e.g. email from your manager about your work allocation, grievance from colleague etc);

We will process information captured within and in relation to instant messaging services that the Company may use from time to time;

We will process and may review information about the use of our IT, communication and other systems to ensure compliance (including your use of Company emails and the telephone system);

We may review your use of public social media (this will only be used in limited situations where a risk to the reputation of the Company and/or misconduct is alleged);

We will process information captured by your use of Company related social media (such as public posts you may make);

We may use photographs of you on our intranet and within Company documentation (where you have agreed);

If you participate in the Company's share option schemes, we may request and process information in relation to the administration of such a scheme;

We will process records relating to your health to explain absence from work, to assess your ability to carry out your role and any support required, and to ensure we comply with legal obligations such as health and safety and the duty to make reasonable adjustments for disabled employees. This will be obtained from your GP or medical adviser or a specialist medical professional appointed by us if required (you will be contacted for consent where we require access to your medical records).

This data is required to effectively manage our employment/working relationship and failure to provide this may prevent us from exercising the contract efficiently. Much of the above data is provided by third parties and other sources (such as colleagues and IT software), however, you are obliged to provide financial information to allow us to pay you and discharge our obligations to HMRC. You are also obliged to provide details of any absence (including holiday and sickness absence) and failure to do so may result in disciplinary action and delay payments to you (such as SSP).