Burke & Clemens Ltd GDPR - Data Protection Policy

Aim and scope of policy
This policy applies to the processing of personal data in manual and electronic records kept by the Company in connection with its human resources function as described below. It also covers the Company's response to any data breach and other rights under the General Data Protection Regulation.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is 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.

The Company makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the Company, the Company will ensure that the third party takes such measures in order to maintain the Company's commitment to protecting data. In line with GDPR, the Company understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Types of data held
Personal data is kept in personnel files or within the Company's HR systems. The following types of data may be held by the Company, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information

- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

Relevant individuals should refer to the Company's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles
All personal data obtained and held by the Company will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes

be adequate, relevant and limited to what is necessary for the purposes of processing

be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay

not be kept for longer than is necessary for its given purpose

be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures

comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures
The Company has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of its data protection systems and procedures
    c. overviewing the effectiveness and integrity of all the data that must be protected.

  There are clear lines of responsibility and accountability for these different roles.

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Company
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Company understands that consent must be freely given, specific, informed and unambiguous. The Company will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences
- it is aware of the implications international transfer of personal data internationally.

Access to data
Relevant individuals have a right to be informed whether the Company processes personal data relating to them and to access the data that the Company holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a subject access request is available from HR. The request should be made to Daniel Clemens.
- the Company will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- the Company will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the Company immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Company will take immediate steps to rectify the information.

For further information on making a subject access request, employees should refer to our Subject access request policy.

Data disclosures
The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data security
The Company adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the Data transfer security policy.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by a Director. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International data transfers
The Company does not transfer personal data to any recipients outside of the EEA.

Breach notification
Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Company becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the Company will do so without undue delay.

Training
New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

Records
The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

Data Protection or Privacy Officer
The company isn't legally required to appoint a Data Protection Officer (DPO) under the GDPR. However, Daniel Clemens, Director has been given responsibility for ensuring that the Company is compliant with the GDPR regulations as the Privacy Officer.

GDRP - Data breach notification policy

Aim and scope of policy
The Company is fully aware of its obligations under the General Data Protection Regulation (GDPR) to process data lawfully and to ensure it is kept securely. We take these obligations extremely seriously and have protocols in place to ensure that, to the best of our efforts, data is not susceptible to loss or other misuse.

The GDPR incorporates a requirement for a personal data breach to be notified to the supervisory authority and in some cases to the affected individuals. This policy sets out the Company's stance on taking action in line with GDPR if a breach were to occur.

Personal data breach
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. A 'breach', for these purposes, is identifiable as a security incident which has affected the confidentiality, integrity or availability of personal data.

As indicated above, a data breach for these purposes is wider in scope than the loss of data. The following are examples of data breaches:

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

Breach detection measures
We have implemented the following measures to assist us in detecting a personal data breach:

- Our staff are trained on how to recognise a personal data breach.
- We understand that a personal data breach isn't only about loss or theft of personal data.
- We have prepared a response plan for addressing any personal data breaches that occur.
- We have allocated responsibility for managing breaches to a dedicated person (Privacy Officer).
- Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

The Company may also become aware of a personal data breach from a member of staff, a client/customer, a member of the public etc.

Notifiable breaches

For the purposes of this policy, a data breach will be notifiable when it is deemed by the Company as likely to pose a risk to people's rights and freedoms. If it does not carry that risk, the breach is not subject to notification although it will be entered on the Company's breach record.

A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

When assessing the likelihood of the risk to people's rights and freedoms, the Company will consider:

- the type of breach
- the type of data involved including what it reveals about individuals
- how much data is involved
- the individuals involved eg how many are involved, how easy it is to identify them, whether they are children etc
- how bad the consequences for the individuals would be and
- the nature of the Company's work and the resultant severity of a breach.

Actions upon identification of breach
When the Company is made aware of a breach, it will undertake an immediate investigation into what happened and what actions must be taken to restrict any consequences. A determination will be made at that point whether the breach is deemed a notifiable breach and whether it is deemed as resulting in a high risk to the rights and freedoms of individuals.

Timescales for notification to supervisory authority
Where a notifiable breach has occurred, the Company will notify the ICO without undue delay and at the latest within 72 hours of it becoming aware of the breach. If notification is made beyond this timeline, the Company will provide the ICO with reasons for this.

If it has not been possible to conduct a full investigation into the breach in order to give full details to the ICO within 72 hours, an initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. The initial notification will be followed up by further communication to the ICO to submit the remaining information.

Content of breach notification to the supervisory authority
The following information will be provided when a breach is notified:

- 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 Privacy Officer 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.

Timescales for notification to affected individuals

Where a notifiable breach has occurred which is deemed to have a high risk to the rights and freedoms of individuals, the Company will notify the affected individuals themselves ie the individuals whose data is involved in the breach, in addition to the supervisory authority. This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

Content of breach notification to the affected individuals
The following information will be provided when a breach is notified to the affected individuals:

- a description of the nature of the breach
- the name and contact details of the Privacy officer 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.

Record of breaches
The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

GDPR - Policy on data subject rights

Aim and scope of policy
The Company processes data for HR purposes concerning job applicants, employees, former employees, workers and contractors. It is fully aware of its obligations under the General Data Protection Regulation (GDPR) to process data lawfully and to ensure that the rights of data subjects, as set out in GDPR, are observed correctly. This policy sets out the rights of the aforementioned individuals as data subjects and the processes which should be followed in the event that the data subject wishes to exercise any such right.

Data subject rights
Under GDPR, you have the following rights in relation to your data:

1. the right to be informed
2. the right of access
3. the right for any inaccuracies to be corrected
4. the right to have information deleted
5. the right to restrict the processing of the data
6. the right to portability
7. the right to object to the inclusion of any information
8. the right to regulate any automated decision-making and profiling of personal data.

1. The right to be informed
You have the right to be told how the Company processes your data and the reasons for the processing. In order to provide this information to you, the Company has a privacy notice to explain what data we collect about you, how we collect and process it, what we process it for and the lawful basis which permits us to process it.

The Company also has a separate privacy notice applicable to job applicants, available at no cost from the Privacy officer.

If the Company intends to use data already collected from you for a different reason than that already communicated, you will be informed of the new reason in advance.

2. The right of access
You have the right to access your personal data which is held by the Company. More information on this is available in the Company's Subject Access Request policy.

3. The right for data to be corrected
One of the fundamental principles underpinning data protection is that the data the Company processes about you will be accurate and up to date. You have the right to have your data corrected if it is inaccurate or incomplete.

If you wish to have your data rectified, you should do so by completing the Data Rectification Form which is available from the Privacy Officer.

The Company will respond to a data rectification request within one month. Where the data rectification request is complex, the Company may extend the timescale for response from one month to three months. If this is the case, the Company will write to you within one month of receipt of the request explaining the reason for the extension.

If the response to your request is that the Company will take no action, you will be informed of the reasons for this and of your right to complain to the Information Commissioner and to a judicial remedy.

Where any data which has been rectified was disclosed to third parties in its unrectified form, the Company will inform the third party of the rectification where possible. The Company will also inform you of the third parties to whom the data was disclosed.

4. The right to have information deleted
You have the right to have your data deleted and removed from our systems where there is no compelling business reason for the Company to continue to process it.

You have a right to have your data deleted in the following circumstances:

- where the personal data is no longer necessary in relation to the purpose for which the Company originally collected or processed it
- where you have withdrawn your consent to the continued processing of the data and there is no other lawful basis for the Company to continue processing the data
- where you object to the processing and the Company has no overriding legitimate interest to continue the processing
- the personal data has been unlawfully processed
- the personal data has to be deleted due to a legal obligation.

If you wish to make a request for data deletion, you should complete the Data Deletion Request form which is available from Oliver Lawton.

Upon receipt of a request, the Company will delete the data unless it is processed for one of the following reasons:

- to exercise the rights of freedom of expression and information
- for the Company to comply with a legal requirement
- the performance of a task carried out in the public interest or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific historical research or statistical purposes or
- the defence of legal claims.

Where your request is not complied with because of the one of the above reasons, you will be informed of the reason. Where your request is to be complied with, you will be informed when the data has been deleted.

Where the data which is to be deleted has been shared with third parties, the Company will inform those third parties where this is possible. However, where this notification will cause a disproportionate effect on the Company, this notification may not be carried out.

5. The right to restrict the processing of data
You have the right to restrict the processing of your data in certain circumstances. Restricting the Company from processing your data means that the Company will continue to hold the data but will stop processing it.

The Company will be required to restrict the processing of your personal data in the following circumstances:

- where you tell the Company that the data it holds on you is not accurate. Where this is the case, the Company will stop processing the data until it has taken steps to ensure that the data is accurate
- where the data is processed for the performance of a public interest task or because of the Company's legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst the Company considers whether its legitimate interests mean it is appropriate to continue to process it
- when the data has been processed unlawfully
- where the Company no longer needs to process the data but you need the data in relation to a legal claim.

If you wish to make a request for data restriction, you should complete the Data Restriction Request form which is available from the Privacy Officer.

Where data processing is restricted, the Company will continue to hold the data but will not process it unless:

- you consent to the processing
- processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, the Company will inform those third parties where this is possible. However, where this notification will cause a disproportionate effect on the Company, this notification may not be carried out.

Where the Company is to lift any restriction on processing, you will be informed in advance.

6. The right to data portability

You have the right to obtain the data that the Company processes on you and use it for your own purposes. This means you have the right to receive the personal data that you have provided to the Company in a structured machine readable format and to transmit the data to a different data controller.

This right applies in the following circumstances:

- where you have provided the data to the Company
- where the processing is carried out because you have given the Company your consent to do so
- where the processing is carried out in order to perform the employment contract between you and the Company
- where processing is carried out by automated means.

If you wish to exercise this right, please speak to the Privacy Officer.

Where a request for data portability is received, the Company will respond without undue delay, and within one month at the latest. Where the request is complex or the Company receives a number of requests, the Company may extend the timescale for response from one

month to three months. If this is the case, the Company will write to you within one month of receipt of the request explaining the reason for the extension.

Where the Company is to comply with your request, you will receive the data in a structured and machine readable form. You will not be charged for the provision of this data. Upon request, the Company will transmit the data directly to another organisation if our IT systems are compatible with those of the recipient.

If the response to your request is that the Company will take no action, you will be informed of the reasons for this and of your right to complain to the Information Commissioner and to a judicial remedy.

The right to portability is different from the right to access. Although both involve a right to access your personal data, the personal data to be accessed is not the same. The right to access your data under the right to portability includes only personal data as described above. Access to data under the right of access includes all personal data relating to you, including that which has not been provided to the Company by you.

7. The right to object to the inclusion of data
You have a right to object to the processing of your data in certain circumstances. This means that you have the right to require the Company to stop processing your data. In relation to your employment with the Company, you may object to processing where it is carried out:

- in relation to the Company's legitimate interests
- for the performance of a task in the public interest
- in the exercise of official authority or
- for profiling purposes.

If you wish to object, you should do so by completing the Data Processing Objection form which is available from the Privacy Officer.

Where you object to processing, the Company will stop the processing activity objected to unless:

- the Company can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights or
- the processing is required in relation to legal claims made by, or against, the Company.

If the response to your request is that the Company will take no action, you will be informed of the reasons.

8. Rights in relation to automated decision making
You have the right not to have decisions made about you solely on the basis of automated decision making processes where there is no human intervention, where such decisions will have a significant effect on you. However, the Company does not make any decisions based on such processes.

If in exceptional circumstances the Company uses special category data, for example, data about your health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership the Company will ensure you have given your explicit consent to the processing or the processing is necessary for reasons of substantial public interest

GDPR - Employee privacy notice

The Company is aware of its obligations under the General Data Protection Regulation (GDPR) and is committed to processing your data securely and transparently. This privacy notice sets out, in line with GDPR, the types of data that we hold on you as an employee of the Company. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

This notice applies to current and former employees, workers and contractors.

Data controller details
The Company is a "Data controller", meaning that it determines the processes to be used when using your personal data. Our contact details are as follows: Burke and Clemens, Diamond House, Jarvis Road, South Croydon, Surrey CR2 6HU.

Data protection principles
In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you
  only use it in the way that we have told you about
  ensure it is correct and up to date
  keep your data for only as long as we need it
  process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed

Types of data we process
We hold many types of data about you, including:

- your personal details including your name, address, date of birth, email address, phone numbers
- your photograph
- gender
- marital status
- dependants, next of kin and their contact numbers
- medical or health information including whether or not you have a disability
- information used for equal opportunities monitoring about your sexual orientation, religion or belief and ethnic origin
- information included on your CV including references, education history and employment history
- documentation relating to your right to work in the UK
- bank details
- tax codes
- National Insurance number
- current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment with us
- letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings

- internal performance information including measurements against targets, formal warnings and related documentation with regard to capability procedures, appraisal forms
- leave records including annual leave, family leave, sickness absence etc
- details of your criminal record
- training details
- CCTV footage
- building entry card records.

How we collect your data
We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in personnel files or within the Company's HR and IT systems.

Why we process your data
The law on data protection allows us to process your data for certain reasons only:

1. in order to perform the employment contract that we are party to
2. in order to carry out legally required duties
3. in order for us to carry out our legitimate interests
4. to protect your interests and
5. where something is done in the public interest.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to:

- carry out the employment contract that we have entered into with you and
- ensure you are paid.

We also need to collect your data to ensure we are complying with legal requirements such as:

- ensuring tax and National Insurance is paid
- carrying out checks in relation to your right to work in the UK
- for thand
- making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of the Company. We have set these out below:

- making decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc
- making decisions about salary and other benefits
- providing contractual benefits to you
- maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises
- offering a method of recourse for you against decisions made about you via a grievance procedure
- assessing training needs
- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- gaining expert medical opinion when making decisions about your fitness for work
- managing statutory leave and pay systems such as maternity leave and pay etc
- business planning and restructuring exercises
- dealing with legal claims made against us
- preventing fraud
- ensuring our administrative and IT systems are secure and robust against unauthorised access

Special categories of data
Special categories of data are data relating to your:

- health
- sex life
- sexual orientation
- race
- ethnic origin
- political opinion
- religion
- trade union membership
- genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

- for the purposes of equal opportunities monitoring
- in our sickness absence management procedures

- to determine reasonable adjustments

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data
We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment.

If you do not provide your data to us
One of the reasons for processing your data is to allow us to carry out our duties in line with your contract of employment. If you do not provide us with the data needed to do this, we will be unable to perform those duties eg ensuring you are paid correctly. We may also be prevented from confirming, or continuing with, your employment with us in relation to our legal obligations if you do not provide us with this information eg confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records or DBS check.

Sharing your data
Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties. This includes, for example, your line manager for their management of you.

We share your data with third parties such as our HR consultants (Madison HR) and our Payroll and accountancy firm in order to maintain personnel records and for administering payment under your contract of employment.

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

We do not share your data with bodies outside of the European Economic Area.

Protecting your data
We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against this such as a data transfer security policy and data breach notification policy.

Where we share your data with third parties, we provide written instructions to them to ensure that your data is held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for. This will be at least for the duration of your employment with us. After the termination of your employment we will retain enough data to respond to references and to meet our legal obligations with regards to income tax and audit purposes which is currently 6 years - personal data that is unlikely to be needed again will be removed from our records upon termination of employment, such as emergency contact details, previous addresses, performance management and health details.

Automated decision making
No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data
The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request. You can read more about this in our Subject Access Request policy.
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may transfer the data that we hold on you for your own purposes
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact the Privacy Officer by email at Daniel.clemens@burke-clemens.co.uk.

Making a complaint

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

GDPR - Data transfer security policy

The Company stores a limited amount of information electronically. This policy governs the procedures to protect this information and sets out how data should be transferred around the Company, and outside the Company, in a secure and protected way.

The law
Data storage is regulated by the Data Protection Act 1998. Standards are set out in the Data Protection Act and one of the key points for consideration in a data transfer situation is that personal data must not be transferred to a country/territory outside the European Economic Area (EEA) unless that country/territory ensures an adequate level of data protection.

Sensitive data
Sensitive data includes data which contains:

- personal details about an individual
- confidential data about the Company
- confidential data about goods, products or services
- confidential data about Company customers and suppliers.

If employees have any doubt as to whether data is or is not 'sensitive data', the employees must refer the matter to Head Office.

Data transfers
Employees must seek consent from the Head Office to authorise the transfer of sensitive data.

Data (sensitive or not) should only be transferred where it is strictly necessary for the effective running of the Company. Accordingly, before any data transfers are requested, the necessity of the transfer should be considered in advance.

After authorisation has been granted, the data must be referred to the Head Office so that it can be encrypted, compressed and password protected before it is sent.

Data transfers by post/courier
Data transfers which occur via physical media such as memory cards or CDs must only be dispatched via secure post. The use of first or second class Royal Mail is not permitted; only Special Delivery or Recorded Delivery should be used. For non-Royal Mail services, a secure courier service must be used with a signature obtained upon delivery.

The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack.

The recipient should be advised in advance that the data is being sent so that they are aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The employee responsible for sending the data is responsible for confirming the data has arrived safely.

Lost or missing data

If an employee discovers that sensitive or confidential data has been lost or is missing, the employee is required to inform the Privacy Officer. An investigation will be initiated immediately to establish the events leading to the data loss/theft.

The Privacy Officer must consider informing any individuals about data loss/theft. This will be necessary if the sensitive data relates to the personal data of individuals which may have been stolen or fallen into the hands of authorised individuals. Informing individuals will be required if there is a risk that the sensitive data has been stolen or sent to the wrong person and will still be necessary even if the data is subsequently located or recovered.

The Privacy Officer must consider referring a matter to the police if it is found that unauthorised individuals have accessed sensitive data. Data which is held in the correct encrypted, compressed and/or password protected formats, which has been accessed by an unauthorised individual, has been accessed unlawfully.

Negligent data transfers
Employees who fail to comply with the requirements of this policy are likely to have their actions considered as gross misconduct, which may result in summary dismissal.

Employees must not be negligent when transferring sensitive data. Examples of negligence include failing to obtain authorisation from the relevant manager, failing to ensure the data is compressed and password-protected data, or using non-secure post services which are not tracked or insured.

GDRP - Subject access request policy

Introduction
Under the General Data Protection Regulation (GDPR), you have a right to receive confirmation that an organisation processes your personal data, and also a right to access that data so that you may be aware of it and are able to verify the lawfulness of the processing. The process for doing so is called a subject access request and this policy sets out the procedure to be undertaken when such a request is made by you regarding data processed about you by the Company.

What is personal data?
"Personal data" is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including your name.

"Special categories of personal data" includes information relating to:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life or
- sexual orientation.

Information you are entitled to
When you make a subject access request, you will be informed of:

- whether or not your data is processed and the reasons for the processing of your data
- the categories of personal data concerning you
- where your data has been collected from if it was not collected from you
- anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards utilised to ensure data security
- how long your data is kept for (or how that period is decided)
- your rights in relation to data rectification, erasure, restriction of and objection to processing
- your right to complain to the Information Commissioner if you are of the opinion that your rights have been infringed
- the reasoning behind any automated decisions taken about you.

Making a subject access request
Subject access requests must be made in writing and can be made in either hard copy format or electronically. The Privacy Officer can provide you with a form for making a request though making a request in this format is not a requirement. Including specific details of the data you wish to see in your request will enable a more efficient response from the Company. We may need to contact you for further details on your request if insufficient information is contained in the original request.

Requests may be made by you personally or by a third party eg a solicitor acting on your behalf. We will request evidence that the third party is entitled to act on your behalf if this is not provided at the same time as the request is made.

Upon receiving a subject access request
The Company will comply with your request without delay and at the latest within one month unless one of the following applies:

- in some cases, we will be unable to supply certain pieces of information that you have requested. This may be because it is subject to legal privilege or relates to management planning. Where this is the case, the Company will inform you that your request cannot be complied with and an explanation of the reason will be provided
- we require extra time because the requests are complex or numerous. In these circumstances, the Company will write to you within one month of receipt of your request to explain why an extension is required. Where an extension is required, information will be provided within three months of the request.

Before supplying the data (where appropriate) we may contact you asking for proof of identity. You must produce this evidence for your request to be complied with.

Your request will normally be complied with free of charge. However, we may charge a reasonable fee if the request is manifestly unfounded or excessive, or if it is repetitive. In addition, we may charge a reasonable fee if you request further copies of the same information. The fee charged will be based on the administrative cost of providing the information requested.

Refusing a request
The Company may refuse to comply with a subject access request if it is manifestly unfounded or excessive, or if it is repetitive. In these circumstances, we will write to you without undue delay and at the latest within one month of receipt to explain why we are unable to comply. You will be informed of the right to complain to the Information Commissioner and to a judicial remedy.

Enforced subject access requests
Forcing employees to obtain information via a subject access request, usually in relation to an individual's criminal record, is a criminal offence. No employee of the Company will be required to make a subject access request.