COMPANY DATA PROTECTION POLICY - GDPR

DEFINITION
This policy sets out how Accuro will handle personal data to ensure compliance with the Data Protection Act 1998 and our adherence to General Data Protection Regulations (GDPR).

SCOPE
The policy covers personal data held on any living individual (employees, sub-contractors, suppliers or customers).

OBJECTIVES
To ensure that Data held and used by Accuro conforms with the Data Protection principles which require that data is:

- Processed fairly and lawfully
- Processed for a limited purpose
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the Data subject's rights
- Secure
- Not transferred to countries outside the European Economic Area (EEA) without adequate protection

PRINCIPLES
Personal data means information (including opinions and intentions) which relates to a living individual and from which he or she can be identified. Such information which identifies an individual and which is being processed by computer and certain information held in manual filing systems.

Employees will expect that data will be held centrally and used by Accuro for employment purposes such as entering into and maintaining the employment contract, the payment of wages, salary and benefits and any statutory or legal obligation.

Every reasonable effort will be made to ensure that information held is secure and remains always correct. However, employees will be requested to assist Accuro by informing their manager in a timely manner of any changes which may occur to personal data.

Information which would be updated would include:

Name	Address	Telephone Number
Next of Kin	Emergency Contact Details	Bank Account Details

The Act requires that certain sensitive data such as ethnic or racial origin and age can only be processed with explicit consent from the employee. Such consent can take various forms and will be asked for at the time the information is requested.

Employees who work with personal data in computer or manual filing systems will be expected always to uphold the principles of the Data Protection Act and to Accuro's practices and policies.

COMPANY DATA PROTECTION POLICY - GDPR

GUIDELINES

These guidelines give more explanation about what all Employees must do to comply with the Act and documents the employee rights as Data Subjects. Finally, there is specific information relevant to the handling of personal data relevant to Line Managers and HR.

What Employees must do

Employees must make sure that they do not obtain personal data or disclose personal data without Accuro's authority. For example, employees must not impersonate another person to obtain personal data. Nor may they disclose personal data, for example to telephone callers, unless they know that they are authorised to make that disclosure.

Employees who as part of their job need to obtain personal data must ensure that the correct data protection notices are given either directly to individuals or to the individuals after they have obtained the data from third parties.

Whenever Employees use personal data they must ensure that their activities stay within those authorised by Accuro. Employees must not start their own collection of personal data without gaining approval from with their manager.

Employees must ensure that any personal data for which they are responsible is accurate and is kept up to date.

Employees must play their part in keeping personal data secure and protected against unauthorised or unlawful processing against accidental loss, destruction or damage.

Employees should not use public (unsecure) WiFi networks to log into our systems or send emails, however, if no secure network is available a 'personal hotspot' should be created using a phone.

Employees should not send emails containing personal data unless the details are held in a password protected file.

Employees should always be mindful of their surroundings when working to ensure that personal data cannot be observed by others.

Employees must not under any circumstances transfer information outside the European Economic area unless they are specifically authorised to do so by Accuro.

The rights of Data Subjects

Data Subjects have the right to apply for a copy of the personal data held about them and information about the processing carried out. If an employee receives any requests (e.g. letter or telephone or face to face), these requests must be passed immediately onto Accuro's Data Protection Officer (HR Director) as there are strict time limits to deal with these requests. Sometimes it may not be obvious that a letter or a complaint also contains a request for information and when in doubt it should be forwarded to Accuro's Data Protection Officer.

Data Subjects have the right to object to processing which they think may cause them substantial damage or distress. They also have a right to prevent processing for direct marketing purposes and a right to object to automated decisions being made about them where those decisions significantly affect them.

If an employee receives any requests that relate to these rights they should pass the objection on to their manager or Accuro's Data Protection Officer immediately.

Individuals also have the right to compensation and to remedies of rectification and erasure for inaccurate data. If you receive claims for any of these remedies again they should be passed to your manager or Accuro's Data Protection Officer as soon as possible.

If you are aware of any practices or procedures that do not comply with the Act's requirements the responsible action is to draw them to the attention of the appropriate manager.

On recruitment

Advertising**:** Individuals providing personal information, even if only name and address, in response to job advertisements should be aware of who they are giving their details to and how it will be used, before they supply their details.

Applications: Information should not be sought from applicants unless it can be justified as being necessary to enable a recruitment decision to be made or for a related purpose such as equality and diversity monitoring. Information should not be sought from all applicants if it is only needed from those who progress further in the recruitment process or from the person appointed. At the time of application, consent should be obtained to any processing of sensitive personal data involved in consideration of the application.

At interview: Limit the recording of responses to questions to those that are relevant to and not excessive for making a recruitment decision. If information is volunteered, only record and retain that which is relevant to the recruitment decision or necessary to be able to demonstrate that the decision was properly taken.

Shortlisting: Shortlisting of job applicants is likely to involve the processing of personal data. It must be undertaken in a way that is fair and lawful.

Retention of recruitment records: Other than for the successful applicant, recruitment records should not be retained any longer than is necessary for making an appointment and responding to any challenges to that appointment. If records are retained because applicants might be considered for other vacancies that arise in the future, applicants should be advised of this and given the opportunity to say no.

Regarding Employee records

Personal records need to be held for staff administration. However, the risk to employees if decisions are taken or opinions formed based on inaccurate or inadequate records are obvious as are the risks if records are not kept securely.

Collection of information: Do not seek personal information from employees that are irrelevant or excessive to the employment relationship.

Maintaining Records: These should be accurate and up to date. Out of date information or information that is no longer required should be deleted.

Sickness Records**:** Sickness records include sensitive data and should be treated as such.

Security: Care should be taken when transmitting employee information by e-mail. Accessing, disclosing or otherwise using employee records without authority may be treated as a serious disciplinary offence and such conduct may constitute a criminal offence.

Probation/Review/Appraisal: Limit the recording of information to that needed to support recent or future employment decisions. Ensure that the record identifies the source of any comments, that opinions are not presented as fact, that information recorded is correct and not misleading and that if the employee has challenged the accuracy this is recorded.

Access & Disclosure

Employees are, at reasonable intervals (which Accuro deems to be every six months) entitled to have access to personal data held on them which is not excluded data (see below) for a fee of £10. They are also entitled to be informed of the purpose for which the data is, or is intended to be, used and the likely recipient.

Once an employee makes a request for confirmation of or sight of data held, which must be in writing, our Data Protection Officer will respond promptly on behalf of Accuro and in any event before the end of 40 days from the date on which the request was received. This is however, conditional upon Human Resources being provided with sufficient information to identify the relevant employee and to locate the information sought.

The following information is excluded from the above:

- Confidential references given or received by Accuro.
- Personal data processed for the purposes of management forecasting or management planning to the extent that disclosure would be likely to prejudice the conduct of that business or activity only.
- Personal data which consists of records of the intentions of Accuro relating to any negotiations with the employee to the extent that disclosure would be likely to prejudice those negotiations only.
- If, to comply with a disclosure request, Accuro would need to disclose information relating to identifiable third party then disclosure is not required unless the third party has consented.

In addition to seeking disclosure of information, an employee is also entitled to request that Accuro does not process data concerning him/her where this will cause or be likely to cause substantial and unwarranted damage or distress, either to the employee concerned or to a third party. Such a request will need to be submitted in writing and where possible, will be agreed to by Accuro. The employee will not be able to prevent processing however, if the processing is necessary for compliance with any legal obligation, it is necessary to protect the vital interests of the employee or is necessary for the performance of a contract to which the employee is a party. Upon receipt of a written request from an employee, our Data Protection Officer will write to the employee within 21 days confirming that the request will be upheld or giving reasons why it will not.

An employee is entitled at any time, by notice in writing, to require a Data Controller to ensure that no decision taken by or on his/her behalf and which significantly affects him/her will be based solely on personal data processed by automatic means.

An employee who feels that he/she has, or is likely to, suffer damage because of either inaccuracy in the data held by Accuro or because of unauthorised disclosure of information must notify a member of Human Resources in writing immediately. Where appropriate, Accuro will correct or erase that information or indicate that the employee contests the information.

Under the Data Protection Act employees have several remedies open to them through the Courts if this policy or their legal rights in respect of personal data are not complied with. In all cases however, employees should submit any complaint in writing to a Data Protection Officer (HR Director) before pursuing any external remedy, they will investigate any such complaint received and, where appropriate, respond to the employee in writing within 21 days.

Regarding Agency & Contract Staff

Records: Apply the same principles/standards to the collection, processing and retention of personal information about contract/agency staff as are applied to employees. This does not mean that the same amount of data needs to be collected as this may be inappropriate and considered excessive.

Security: If contract/agency staff have access to employee records and other personal data have in place a written contract with them to tie them to only processing the data in accordance with instructions they are given and to keeping the data secure.

Medical Testing

Types of testing: Medical testing includes drug testing, alcohol testing, as well as more general medical testing.

Testing employees: Testing should only occur where it is part of a health and safety programme operating in the interests of employees or it is a necessary and proportionate measure to: prevent a significant risk to the health and safety of the employee or others; to determine the employee's fitness for continued employment or to determine the employee's entitlement to health related benefits e.g. sick pay.

Discipline & Dismissal

Accuracy: To be compliant with the Act the accuracy of information is crucial, especially if, as in this case, it is to form the basis of disciplinary action. Ensure that when employment is terminated both Accuro and the employee are clear about the basis/reason for the termination and that this is accurately recorded.

Security: It is important that any allegations that may lead to disciplinary action (for example claims of harassment) is crucial to avoid prejudice that can be caused even if the case is ultimately unfounded, to protect both the complainant and the accused party.

Holding records: Disciplinary procedures provide for warnings to "expire" after a set period. Ensure that what is meant by "expire" is clear and take the necessary action at the appropriate time.

Retaining records

Information should not be kept for longer than is necessary but equally it should not be discarded when doing so would render the record inadequate. Where specific legal provisions require the retention of employment records for a set period then this is the minimum time for which they should be retained. Information should not be retained simply on the basis that it might come in useful one day. Ensure that records that are no longer required are properly and securely disposed of.

In the absence of a specific business case supporting longer retention periods the following shall be used:

Type of record	***Retention period***
Application form/Data Information	Duration of employment
References received	1 year
Payroll and tax information	3 years
Sickness records	3 years
Annual leave records	3 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	3 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given	5 years from reference/end of employment

Summary of record of service e.g. Name, position held, dates employed	6 years from end of employment
Records relating to accident or injury at work	6 years

Accuro has appointed the role of HR Director as its Data Protection Officer, to whom, in the first instance, all enquiries relating to the interpretation of this policy as well as holding of personal data should be referred.

GENERAL DATA PROTECTION REGULATIONS (GDPR) - POLICY

This Policy sets out the basis on which Accuro will process personal information provided (personal data).

Accuro takes its obligations in respect of the privacy of personal information very seriously and we will only process personal information as detailed in this policy unless we inform you otherwise. To ensure that the personal information we hold is accurate and up-to-date, we request that you inform us of any relevant changes to the personal information we hold about you.

The person responsible for data protection within our organisation is our HR Director (Patrick White) who can be contacted at DPO@accurofacilities.co.uk.

If you do not wish us to process personal information in accordance with this policy, then please do not provide it to us. Please refer to Section 4 'Your rights', in respect of data that we already hold, or which we receive from third parties.

SECTION 1: EMPLOYEES

The personal data we collect, receive, hold and process includes the following as applicable:

- Name
- Address
- Email and other contact details
- Date of birth
- Educational history, qualifications & skills
- Visa and other right to work or identity information
- Passport and or Driving Licence
- Bank details
- National insurance and tax (payroll) information
- Next of kin and family details
- Contact details of referees
- Information contained in references and pre-employment checks from third parties
- Other sensitive personal information such as health records (see 'Sensitive Personal Data')
- Photograph

We may obtain your personal data from the following sources (please note that this list is not exhaustive):

- You (e.g. a Curriculum Vitae, application or registration form)
- A client
- Interview
- Conversations on the telephone (which may be recorded)
- Notes following a conversation or meeting
- Umbrella bodies responsible for Disclosure and Barring Service (DBS)

How we will use your personal data:

The processing of your personal information may include:

- Collecting and storing your personal data, whether in manual or electronic file within the company HR and Payroll systems
- Assessing and reviewing your suitability for job roles within Accuro

- Engaging you for a role with us, including any related administration e.g. timesheets and payroll
- Sending legislative required information to third parties with whom we have or intend to enter into arrangements which are related to our recruitment process
- Providing information to regulatory authorities or statutory bodies, and our legal or other professional advisers including insurers
- Establishing quality, training and compliance with our obligations and best practice
- For the purposes of backing up information on our computer systems

Why we process your personal data:

1. ***Employment Contract*** - To provide our services, we may enter into a contract with you and/or a third party and will need certain information, for example your name and address. A contract will also contain obligations on both your part and our part and we shall process your data as is necessary for those obligations.

2. **Legal Obligations** - We must comply with several statutory provisions, which necessitate the processing of personal data, which amongst other things requires us to:
   - Verify your identity
   - Assess your suitability for a job role
   - Maintain records for specific periods

   We are also required to comply with statutory and regulatory obligations relating to business generally, for example complying with tax, bribery, fraud/crime prevention and data protection legislation, and co-operating with regulatory authorities such as HMRC.

3. ***Business Requirements*** - In providing our services, we will carry out some processing of personal data which is necessary for our legitimate interests, which include:
   - Retaining records of our dealings and transactions and where applicable, use such records for the purposes of:
     - establishing compliance with contractual obligations between company and staff
     - addressing any query or dispute that may arise including establishing, exercising or defending any legal claims
     - protecting our reputation
     - maintaining a back-up of our system, solely for being able to restore the system to a point in the event of a system failure or security breach
     - evaluating quality and compliance including compliance with this Privacy Notice
     - determining staff training and system requirements
     - assess suitability and contact within our service
     - source potential opportunities or roles

   This means that for our commercial viability and to pursue these legitimate interests, we may continue to process your personal data for as long as we consider necessary for these purposes.

Consent to our processing of your data:

We may process your personal data on the basis that you have consented to us doing so for a specific purpose. For example, information provided in respect of applying for a role.

You may withdraw your consent to our processing of your personal information for a purpose at any stage. However, please note that we may continue to retain, or otherwise use your personal information thereafter where we have a legitimate interest or a legal or contractual obligation to do so.

Sensitive Personal Data (SPD)

Sensitive personal data is information which is intensely personal to you and is usually irrelevant to our consideration of your suitability for a role within our recruitment process. Examples of SPD include information which reveals your political, religious or philosophical beliefs, sexual orientation, race or ethnic origin, or information relating to your health.

Regardless of the basis for your dealings with us, we request that you do not provide us with any sensitive personal data unless necessary. However, to the extent that you do provide us with any sensitive personal data, such as data which you choose to share with us in conversation, we shall only use that data for the purposes of our relationship with you or for the provision of our services. This will be for one or more of the following reasons:

- You have explicitly consented to the processing
- For our assessment of your suitability for job roles or working capacity
- Where processing is necessary for obligations or rights under employment, social security or social protection law
- To maintain records of our dealings to address any later dispute, including but not limited to the establishment, exercise or defence of any legal claims

Who we share personal data with:

We shall not share your personal information unless we are entitled to do so. The categories of persons with whom we may share your personal information include:

- Contract provision of personal data variation subject to Transfer of Undertakings
- Any regulatory authority or statutory body pursuant to a request for information or any legal obligation which applies to us
- Parties who process data on our behalf, which may include:
  - Selima or Access Group of companies
  - Ucheck
  - Legal and professional advisors
  - Insurers

Automated decisions

We do not use any automated decision making software.

SECTION 2: THIS SECTION APPLIES TO ALL PERSONAL DATA

Transfer

In the event of a sale, merger, liquidation, receivership or the transfer of all or part of our assets or business to a third party, we may need to transfer your information to a third party. Any transfer will be subject to the agreement of the third party to this Privacy Notice and any processing being only in accordance with this Privacy Notice.

Data Security and Confidentiality

It is our policy to ensure, in so far as is reasonably practicable, that our systems and records are secure and not accessible to unauthorised third parties in line with best practice.

Retaining your data

It is our policy to only store your personal data for as long as is reasonably necessary for us to comply with our legal obligations and for our legitimate business interests. If, however you believe that we should delete your personal data, please inform us in writing of your reasons. Please see Section 3 'Your Rights' below.

Changes to this Privacy Notice

This Privacy Notice is regularly reviewed and may be updated from time to time to reflect changes in our business, or legal or commercial practice.

SECTION 3: YOUR RIGHTS

We take the protection of your personal data very seriously and it is important that you know your rights within that context, which include rights to:

- Request a copy of the personal data that we hold
- Object to our processing of your data where that processing is based upon legitimate interest and there are no compelling grounds for the continued processing of that data
- Request that we restrict processing of your data in certain circumstances
- Request that data is erased where the continued use of that data cannot be justified
- Withdraw your consent to our processing of your personal data for a purpose at any stage. However, please note that we may continue to retain, or otherwise use your personal information thereafter where we have a legitimate interest or a legal or contractual obligation to do so. Our processing in that respect will be limited to what is necessary in furtherance of those interests or obligations
- Request that inaccurate or incomplete data is rectified
- Please note that should you exercise your right to request that we erase data or cease any processing activity, we may retain a record of this request and the action taken to both evidence our compliance, and to take steps to minimise the prospect of any data being processed in the future should it be received again from a third-party source.

If you have any questions concerning your rights, should you wish to exercise any of these rights, or if you are dissatisfied about any aspect of the way in which your data is processed please contact Accuro's Data Protection Officer at DPO@accurofacilities.co.uk

This does not affect your right to make a complaint to the Information Commissioner's Office.