General Data Protection Regulations (GDPR) Policy

Pickerings®

1.0 INTRODUCTION

Any organisation which processes any personal data (whether that personal data is held in a paper or electronic format e.g. on computers, laptops, smartphones, electronic networks, CDs, USBs etc.) must comply with the European Data Protection Directive (95/46/EC) (the "Directive"), which is implemented in the UK by the Data Protection Act 2018 (the "Data Protection Laws"). Accordingly Pickerings Hire Ltd and its group companies and each employee must comply with the Data Protection Laws.

To help achieve compliance with the Data Protection Laws, this policy sets out what the Company and each staff member needs to do when processing personal data. The types of personal data that the Company may typically be required to handle include details of current, past and prospective employees as well as personal data about other individuals (such as consultants and suppliers and shareholders that we may communicate with from time to time).

2.0 SCOPE

This policy applies to all staff members. For the purposes of this policy, "staff member" means all of the company's permanent and temporary employees, and any other individuals who are working for the Company but are not directly employed, (including officers, consultants, contractors, interns and agency workers). Use of the term "staff member" shall not be taken to imply that any particular individual has employment status with the company.

This policy does not form part of any employee's contract of employment and it may be amended at any time. The company will notify staff if changes are made to this policy.

If there is anything in this policy which is not understood or there are any questions, please contact the IT Director for assistance.

3.0 PRINCIPLES

3.1 Consequences of Breaching the Data Protection Laws and this Policy

Serious breaches of the Data Protection Laws can result in enforcement action by the Information Commissioner against the Company and in significant fines (of up to £500,000) being imposed on it. Data protection laws in the EEA are likely to change in the near future, since a new EEA Data Protection Regulation is expected to replace the existing Directive. The Regulation will mean even more stringent compliance obligations and even bigger fines for data protection breaches (up to 5% of annual global turnover). Further, some breaches of the Data Protection Laws are a criminal offence. Consequently any breach of this policy will be taken seriously and may result in disciplinary action, in line with the Company Disciplinary Policy.

3.2 Terms used in the Data Protection Laws and in this Policy

This section gives definitions of the terms used in the Data Protection Laws and which are used in this policy.

Term	Definition
Personal Data	Means information from which a *living individual* can be identified. This includes factual information such as telephone numbers, names, addresses, e-mail addresses, photographs, CCTV footage and voice recordings. It also includes expressions of opinion and indications of intentions about individuals (and their own expressions of opinion/intentions), such as performance appraisals. Information which does not, *on its own,* identify an individual is still 'personal data' for the purposes of the Data Protection Laws if it can be combined with other information that the company holds or that it could obtain fairly easily. For example, if personal data has been anonymised by the company but it also holds the key to 'de-anonymise' the information or could fairly easily obtain that key, then the anonymised information will still be personal data for the purposes of the Data Protection Laws.
Sensitive Personal Data	Information relating to: • racial or ethnic origin; • political opinions; • religious beliefs or beliefs of a similar nature; • trade union membership; • physical or mental health or condition; • sexual life; or • offences or alleged offences or information relating to any proceedings for offences committed or allegedly committed.
Processing	The term 'processing' covers virtually anything that can be done with personal data (whether processed in an electronic format or in a structured paper-based format), including: • obtaining, recording, retrieving, consulting or holding it; • organising, adapting or altering it; • disclosing, disseminating or otherwise making it available; and • aligning, blocking, erasing or destroying it.
Data Subject	This is the individual to whom the personal data relates.
Data Controller	A party who (either alone or jointly) determines the *purposes* for which, and the *manner* in which, any personal data is, or will be, processed. The Company is a data controller.
Data Processor	A party who processes personal data on behalf of a data controller (other than an employee of the data controller). For example, some of the company's suppliers (such as estate agents) are data processors for the Company.
European Economic Area or "EEA"	Means European Union member states plus Norway, Liechtenstein and Iceland.

EIGHT DATA PROTECTION PRINCIPLES

1	Personal data must be processed fairly and lawfully;
2	Personal data must be obtained for one or more specified and lawful purposes and must not be processed incompatibly with those purposes;
3	Personal data must be adequate, relevant and not excessive in relation to the purposes for which the data are processed;
4	Personal data must be accurate and kept up to date;
5	Personal data must not be kept for longer than is necessary;
6	Personal data must be processed in accordance with the rights of the data subjects under the Data Protection Laws;
7	Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data as well as against accidental loss, destruction of or damage to that data; and
8	Personal data must not be transferred outside of the EEA unless the recipient provides an adequate level of protection in line with the Data Protection Laws.

4.0 PROCEDURE

4.1 How to Process Personal Data Fairly and Lawfully (Principles 1 and 2)

To process personal data fairly, employees need to make sure that they only process personal data if the data subject has been told:

- who the data controller is (in this case the Company);
- the purpose for which the data is to be processed by the Company; and
- the identities of anyone to whom the data may be disclosed or transferred.

This information is contained in so-called "privacy notices" which are given to staff members, applicants and any other individuals about whom the company process personal data. Staff must ensure that they do not process personal data for any purpose other than those contained in this policy

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Data Protection Laws. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before carrying out any new processing (except in certain circumstances where a legal exemption from this obligation applies).

Staff should only collect the minimum amount of personal data necessary for their purpose. In particular, please be cautious when inputting information about individuals into CRM systems/contacts databases. Do not include information that is not required, e.g. notes/observations about an individual, because this could go beyond the purpose for which the data was originally collected and may result in a claim against the company for unlawful processing of personal data.

To process personal data lawfully, the Company must meet certain conditions that are set out in the Data Protection Laws. Those conditions which are most relevant to the company as an organisation are summarised in Tables A and B below.

One of the conditions for processing personal data is that the data subject has given their consent to such processing. Relying on consent to process personal data may be appropriate in some circumstances, but it must be kept in mind that if other conditions are relevant they should be relied on instead – in other words, consent is a condition of 'last resort'. Also note that the consent must be fully informed (i.e. the data subject knows what they are consenting to), and the data subject must have a genuine choice as to whether to give consent or not.

IMPORTANT

When processing **non-sensitive personal data**, staff must make sure that **at least one of the conditions in Table A** applies.

When processing **sensitive personal data**, **staff must ensure that one of the conditions in Table A applies and at least one of the conditions in Table B also applies**. The conditions in Table B are fairly limited, so when processing sensitive personal data it is likely that the company will need to get written consent from the data subject to the processing of their sensitive personal data.

TABLE A – Key conditions for processing <u>any</u> personal data (one or more must apply)

Business Interests	Processing is carried out in order to pursue the Company's legitimate business interests (e.g. collecting personal data from customers/clients so that the Company can deliver its projects/services). Much of the processing of personal data that the Company does as an organisation falls under this condition. This condition only applies if the processing does not adversely affect the individual concerned. If there is a serious mismatch of competing interests between the business and the individual, the individual's interests will have priority over business interests.
Contracts	Processing is carried out in order to enter into a contract between the Company and the data subject or to perform such a contract.
Legal Obligations	Processing is carried out in order to comply with legal obligations placed on the Company. This does not apply to contractual obligations.
Vital Interests of Data Subject	Processing is carried out in order to protect the data subject's vital interests (e.g. where an individual's personal data needs to be disclosed in a medical emergency).

TABLE B – Key conditions for processing sensitive personal data (one or more must apply)

Employment Obligations	Processing is carried out as part of the Company exercising its legal obligations or rights in connection with employment such as sick pay administration, or checking that an individual is eligible to work in the UK.
Equal Opportunities	Processing is carried out in order to monitor equal opportunities within the company.
Legal Rights	Processing is carried out in order to establish, exercise or defend the legal rights of the Company.
Publicly Available Information	The personal data has been made public as a result of steps deliberately taken by the data subject. Be cautious where relying on this condition – information available publically such as on the internet, may not have been made public by the data subject themselves (in which case this condition would not apply).
Vital Interests of Data Subject	Processing is carried out in order to protect the data subject's vital interests (e.g. where an individual's sensitive personal data needs to be disclosed in a medical emergency).

4.2 How to Ensure Processing is Adequate, Relevant and not Excessive (Principle 3)

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any personal data which is not necessary for that purpose should not be collected in the first place.

As well as ensuring that any personal data which is processed is necessary and relevant for the purpose for which it is being processed, staff must at the same time ensure that they have adequate personal data for their purpose. In other words, enough information should be obtained about an individual to enable them to perform their purpose(s) but no more.

4.3 How to Keep Personal Data Accurate and Up to Date (Principle 4)

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date personal data should be destroyed or erased from the systems.

Although ultimately it is the Company's responsibility to ensure personal data is up to date and accurate, it will often be reliant on data subjects themselves to advise of changes to their personal data. From a practical perspective it is often useful to encourage data subjects to make contact if personal data held about them becomes out-of-date or if they are aware of any inaccurate data being held about them.

If staff are involved in planning an activity or project that includes processing of personal data, they should think about appropriate methods that can be implemented easily to encourage data subjects to notify the company about changes to their personal data.

4.4 How to Ensure Personal Data is not Kept for Longer than Necessary (Principle 5)

Personal data should not be kept longer than is necessary for the purpose for which it was obtained. This means that personal data should be destroyed or erased from the Company's systems when it is no longer required.

As the Data Protection Laws do not prescribe any specific minimum or maximum retention periods which apply to personal data, staff will need to make decisions about how long to keep certain types of personal data on a case by case basis. It may also be the case that they will need to consider whether there are any data retention practices and procedures that are specific to their department, and with which they will need to comply. If unsure about whether certain personal data should be retained, staff should contact the HR Department.

4.5 How to Process Data in Accordance with Data Subjects' Rights (Principle 6)

Data Subjects are granted various rights by the Data Protection Laws. The key rights and the actions that need to be taken when they are exercised are as follows:

4.5.1 The right to ask to see what personal data the company holds about them

Any written requests received from staff members, former staff members and potential recruits should be referred to the HR Department and written requests from any other individuals to the HR Department immediately, as the Company has only up to 40 days in which to respond to requests.

Sometimes requests for personal data may be made over the telephone – in which case staff should:

- check the caller's identity to make sure that information is only given to a person who is entitled to it;
- ask the caller to put their request in writing if they are unsure about the caller's identity and where their identity cannot be checked; and
- refer to their line manager or to the HR Department for assistance in difficult situations. No-one should be bullied into disclosing personal data.

4.5.2 ***The right to require the Company to rectify any personal data which is inaccurate***

For example, if a staff member is requested to change an address of a customer/client or supplier etc. they should make those changes immediately. If inaccurate personal data about a data subject has been passed on to a third party, it may also be necessary to correct the third party's data, depending on the nature of the data and whether the third party is still likely to be using it. If the personal data is of a more serious nature, a record of the change made must be kept and circumstances in which it was made and if it is felt necessary, the line manager spoken to.

4.5.3 ***The right to prevent processing of their personal data if this has caused or is likely to cause damage or distress***

Please contact the HR Department if a request is received to prevent processing.

4.5.4 ***The right to ask for the logic involved in any automated decision taken without human input (i.e. by a computer)***

The HR Department should be contacted if such a request is received.

4.5.5 ***The right to prevent the company sending unsolicited marketing materials to them***

Depending on the type of unsolicited marketing, intended recipients may have a right to either opt-in or opt-out.

4.6 What Security Measures must be Complied with (Principle 7)

Personal data must be kept secure from unauthorised access and from being accidentally lost, destroyed or damaged. To do this, staff should follow all applicable Company security guidelines and procedures and all policies that have a bearing on data security such as the Company's IT Acceptable Use Policy and Confidential Data Policy.

Personal data should not be disclosed to a third party (i.e. a person or organisation) unless one or more of the following apply:

- either the data subject has been informed in a privacy notice that his or her personal data may be disclosed to such parties and the purpose for which it is being disclosed, or the disclosure takes place in the course of conducting Company's legitimate business activities and the data subject would expect their personal data to be used for this purpose;
- the disclosure is made with the consent of the data subject to whom the personal data relates. If sensitive personal data is being disclosed, written consent to disclosure must be obtained;
- a senior officer of the company has authorised the disclosure;
- the disclosure will be to an organisation and/or individual entitled to receive the personal data, for example, to the police where the information is necessary to prevent or detect crime, or to the tax authorities;
- the disclosure is made in order to comply with legal obligations placed on the Company or to comply with a court order; or
- the disclosure is made in the course of legal proceedings.

Any disclosure of personal data must be subject to appropriate security safeguards and, depending on the nature of the personal data, confidentiality obligations. In particular, any internal communications about a staff member's salary, benefits or any other information about Company staff members should be communicated securely and in confidence.

If the disclosure is to a third party that provides services to the Company, only such personal data as is necessary should be disclosed, and a 'Data Processor Agreement' should be put in place with that third party. A Data Processor Agreement ensures that the third party is contractually obliged to comply with legally-specified minimum data protection requirements and to put appropriate security measures in place. The HR Department should be contacted for proposed Data Processor Agreement wording. If it is intended to make use of a Data Processor Agreement with a third party, it should be confirmed with the HR Department whether any amendments need to be made to the Agreement to reflect the specific circumstances.

If anyone is uncertain about disclosing any personal data to third parties they should contact the HR Department for guidance.

4.7 When can Personal Data be Transferred Outside the EEA? (Principle 8)

Personal data should not be transferred to a country outside of the EEA (European Economic Area) unless:

- it is to perform a contract with the data subject;
- the data subject has consented;
- the country is on the Information Commissioner's approved countries list;
- the personal data is being sent to a US- based organisation which is compliant with 'Safe Harbor' provisions; or
- a contract has been put in place with the third party/third parties to which the personal data will be transferred, based on European Commission approved standard contracts for transfers of personal data outside of the EEA (known as “Model Contracts”).

Note that a transfer of personal data outside of the EEA not only includes sending relevant data to an entity in a non-EEA country (e.g. by email) but also includes allowing access to that data. For example, where a group company is granted access to personal data on servers in the EEA, and the data is then accessible by individuals in a non-EEA country, this is considered to be a transfer of data to that non-EEA country.

If anyone is unsure about whether a 'transfer' of personal data will take place, or are uncertain about transferring personal data outside of the EEA generally, they should contact the HR Department.

Signed:

Neil Moss
Managing Director
April 3rd 2024