FOREMAN ROBERTS DATA PROTECTION POLICY

Foreman Roberts Consulting Limited ('the company'; 'we'; 'us' or 'our') is committed to ensuring that your privacy is protected. We will comply with the principles of the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) and aim to maintain best-practice standards in our processing of personal and sensitive personal/company data.

Foreman Roberts Consulting Limited will be transparent about how it collects and uses personal data and meeting its data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

We have appointed Andrew Pemberton, Finance Director as the person with responsibility for data protection compliance within the company. He can be contacted at apemberton@foremanroberts.com. Questions about this policy, or requests for further information, should be directed to him.

Definitions
"Personal data" is any information that relates to an individual who can be identified from that information.

"HR-related personal data" is personal data of job applicants, employees (which for this purpose includes contractors and sub consultants) and former employees.

"Processing" is any use that is made of data, including; collecting, storing, amending, disclosing or destroying it, whether the data is stored electronically on paper or on other materials.

"Special categories of personal data" means information about an individual's racial or ethnic origin, religious or philosophical beliefs, trade union membership and health life or sexual orientation.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles
We process HR-related personal data in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent manner.
- Confidentiality of personal data will be assured.
- We collect personal data only for specified, explicit and legitimate purposes.
- We processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep information that we believe is up-to-date.
- We keep personal data only for the period necessary for processing.
- We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful access/ processing, and accidental loss, destruction or damage.

Information regarding the collecting, processing and holding of personal data of individuals gathered during employment (or the contract) is contained in privacy notices issued to individuals. Personal data of individuals will only be processed for reasons stated in the privacy notice.

For any processing activity we undertake, the purpose of the activity being carried out will be reviewed and we will select the most appropriate lawful basis for that processing in accordance with GDPR.

Where the company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with GDPR guidelines or is anonymised.

We will update personal data promptly if an individual advises that their information has changed or is inaccurate.

The company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of GDPR.

Individual rights
We recognise that individuals have rights under GDPR in relation to their personal data. We will take all reasonable steps to protect these rights.

Individuals are made aware of their rights in the Privacy Notice which employees receive at the same time as their Contract of Employment. Employees at the time GDPR legislation was introduced in May 2018 received an Employee Privacy Notice. Contractors/consultants and other individuals that carry out work for us will receive a Privacy Notice when we first ask for any form of personal information. Job applicants will receive a Privacy Notice should we take their application further.

Data security
The company takes the security of HR-related personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by authorised staff in the proper performance of their duties.

All data is duplicated across each server to alternate disk drives to provide a security copy. All data is further backed up to external hard drives.

Where the company engages third parties to process personal data on its behalf, such as for payroll and pension, they do so, on the basis of written instructions and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

International data transfers
HR related personal data may be transferred to countries within the EU and outside the EEA to support international projects and manage international transfers. Such data transfers are carried out once confirmation is received that the company the data is being transferred to will abide by the principles of GDPR.

Individual responsibilities
Individuals are responsible for helping the company keep their personal data up to date. Individuals should let our HR Manager, Caroline Hooper, know if data provided to the company changes, for example if an individual moves house or changes their bank details.

Individuals may have access to the personal data of other individuals and our clients in the course of their employment/contract. Where this is the case, the company relies on individuals to help meet its data protection obligations to staff and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the company) who have appropriate authorisation;
- to keep data secure;
- not to remove personal data, from the company's premises without adopting appropriate security measures (such as password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices; and
- to contact the person with responsibility for data protection compliance if they are unsure of any aspect of data protection.

Failing to comply with these requirements may amount to a disciplinary offence, which will be dealt with under the company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or client data without authorisation or a legitimate reason to do so, may be considered gross misconduct and could lead to dismissal without notice.

Training
The company will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy will receive training to help them understand their duties and how to comply with them.

Client and Other Party Data
Personal data of clients and other parties is limited and is held under the lawful basis of "legitimate interest".

Data held is usually limited to an individual's name, phone number, company e-mail address and company address. Additional data will be held if it is provided to us by that individual. This data is gathered in the course of business in several ways including; exchanging business cards and e-mails; the exchange of information across project teams whilst working on projects and is held only for the purposes of conducting business.

Our uses of personal data include:

- inviting people to events;
- informing people about our projects; and
- sending people updates on Company issues.

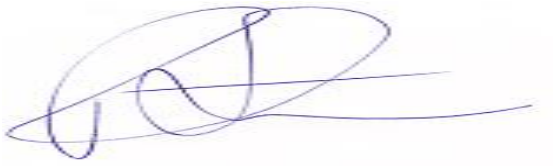
A client or other party can ask for their details to be removed at any time. On receipt of such a request their details will be removed from our systems and they will not be contacted again.

All our mail shots have a link to this Data Protection Policy and an unsubscribe 'button'. Should an individual unsubscribe they will no longer receive information from us.

Those visiting the Company web site
The Company uses Google Analytics to gather metrics for the company web site. The data gathered is aggregated data and does not as such identify individuals.

Data Protection Breaches
If you feel the Company has misused information or hasn't kept data secure, the incident should be reported to the person with responsibility for data protection, Andrew Pemberton, immediately, giving full and accurate details of the incident in writing. Andrew will thoroughly investigate and provide future guidance.

Policy Review
This policy will be reviewed as and when required (annually, as a minimum) and updated if required in accordance with our data protection obligations.



Signed: Roy Steptoe CEO