DATA PROTECTION AND BRIBERY POLICY

INTRODUCTION

The General Data Protection Regulation (GDPR) protects employees against the misuse of personal data and may cover both manual and electronic records. All records held on computer fall within The General Data Protection Regulation (GDPR). Certain manual files may also fall within the Act, depending on the ease of access to data within the file. However, for consistency and good practice, Hackle Security Services Ltd *(The Company)* will adopt the same approach for data held.

The Act requires that any personal data held should be:

- ✓ Processed fairly and lawfully.
- ✓ Obtained and processed only for specified and lawful purposes.
- ✓ Adequate, relevant and not excessive.
- ✓ Accurate and kept up to date.
- ✓ Held securely and for no longer than is necessary.
- ✓ Not transferred to a country outside the European Economic Area unless there is an adequate level of data protection in that country.

The Act also gives employees certain rights. For employment purposes, the most important right is the right to access the personal data held about the employee.

PURPOSE(S) FOR WHICH PERSONAL DATA MAY BE HELD

Personal data relating to employees may be collected primarily for the purposes of;

- ✓ Recruitment, promotion, training, redeployment and/or career development.
- ✓ Administration and payment of wages.
- ✓ Calculation of certain benefits including pensions.
- ✓ Disciplinary or performance management purposes.
- ✓ Performance review.
- ✓ Recording of communication with employees and their representatives.
- ✓ Compliance with legislation.
- ✓ Provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers.
- ✓ Staffing levels and career planning.

The Company considers that the following personal data falls within the categories set out above;

- ✓ Personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant.
- ✓ References and CVs.
- ✓ Emergency contact details.
- ✓ Notes on discussions between management and the employee.
- ✓ Appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment.
- ✓ Training records.
- ✓ Salary, benefits and bank/building society details.
- ✓ Absence and sickness information.

Employees or potential employees will be advised by the Company of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed. The Company will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

SENSITIVE PERSONAL DATA

Sensitive personal data includes information relating to the following matters;

- ✓ The employee's racial or ethnic origin.
- ✓ His or her political opinions.
- ✓ His or her religious or similar beliefs.
- ✓ His or her trade union membership.
- ✓ His or her physical or mental health or condition.
- ✓ His or her sex life.
- ✓ The commission or alleged commission of any offence by the employee.

To hold sensitive personal data, the Company must additionally satisfy a sensitive data condition. The most appropriate condition for employment purposes is that the processing is necessary to enable the Company to meet its legal obligations (for example, to ensure health and safety or to avoid unlawful discrimination).

RESPONSIBILITY FOR PROCESSING OF PERSONAL DATA

The Company will appoint a Data Controller as the named individual responsible for ensuring all personal data is controlled in compliance with The General Data Protection Regulation (GDPR). Employees who have access to personal data must comply with this Policy and adhere to the procedures laid down by the Data Controller. Failure to comply with the Policy and procedures may result in disciplinary action up to and including summary dismissal.

Employees who have access to personal data must comply with this Policy and adhere to the procedures laid down by the Data Controller. Failure to comply with the Policy and procedures may result in disciplinary action up to and including summary dismissal.

USE OF PERSONAL DATA

To ensure compliance with The General Data Protection Regulation (GDPR) and in the interests of privacy, employee confidence and good employee relations, the disclosure and use of information held by the Company is governed by the following conditions;

- ✓ Personal data must only be used for one or more of the purposes specified in this Policy.
- ✓ Company documents may only be used in accordance with the statement within each document stating its intended use and provided that the identification of individual employees is not disclosed; aggregate or statistical information may be used to respond to any legitimate internal or external requests for data *(e.g., surveys, staffing level figures)*.
- ✓ Personal data must not be disclosed, either within or outside the Company, to any unauthorised recipient.

PERSONAL DATA HELD FOR EQUAL OPPORTUNITIES MONITORING PURPOSES

Where personal data obtained about candidates is to be held for the purpose of Equal Opportunities monitoring, all such data must be made anonymous.

DISCLOSURE OF PERSONAL DATA

Personal data may only be disclosed outside the Company with the employee's written consent, where disclosure is required by law or where there is immediate danger to the employee's health.

ACCURACY OF PERSONAL DATA

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date. In order to ensure the Company's files are accurate and up to date, and so that the Company is able to contact the employee or, in the case of an emergency, another designated person, employees must notify the Company as soon as possible of any change in their personal details *(e.g., change of name, address; telephone number; loss of driving licence where relevant; next of kin details, etc).*

ACCESS TO PERSONAL DATA

Employees have the right to access personal data held about them. The Company will arrange for the employee to see or hear all personal data held about them within one month of receipt of a written request and this request maybe subject to a £10.00 administration fee.

THE BRIBERY ACT

THE OFFENCES

1. A general offence of "offering, promising or giving of a bribe"- known as "active bribery"
2. A general offence of "the requesting, agreeing to receive or accepting of a bribe" – known as "passive bribery"
3. There is also an offence specific to bribing a foreign public official
4. The corporate liability of "failing to prevent bribery on behalf of a commercial organisation"

HOW THIS MAY EFFECT YOU!

"OFFERING, PROMISING OR GIVING OF A BRIBE" – KNOWN AS "ACTIVITY BRIBERY"

1. If you were to promise to or actually bribe a member of the client's staff to get sensitive information from them to then pass on to a third party.
2. If you were to promise to or actually bribe another contractor (e.g. cleaner, engineer etc) for them to pass information on that they might have access to.
3. Offering to, promise to or actually bribing someone to "look the other way" whilst you illegally accessed information that you were not entitled to see.

"THE REQUESTING, AGREEING TO RECEIVE OR ACCEPTING OF A BRIBE" – KNOWN AS "PASSIVE BRIBERY"

1. Asking for, agreeing to accept or actually taking a bribe to then provide confidential client information to a third party (e.g. a competitor of the client, customer or own company).
2. Asking for, agreeing to accept or actually taking a bribe to "look the other way" and allow unauthorised access to the building or an area within the building for a third party to steal our clients information or property.

PENALTIES ON CONVICTION:

1. Individuals – up to 10 years in prison and/or an unlimited fine
2. Proceeds of the bribe confiscated
3. Companies – unlimited fine
4. Directors – up to 15 years in prison
5. Possible exclusion from public sector contract opportunities
6. Irreparable brand and reputational damage

WHAT SHOULD YOU DO:

1. **NEVER** say yes to accepting a bribe.
2. **NEVER** agree to pay or offer a bribe.
3. Use the company whistle blowing policy if you suspect a colleague may have been compromised.
4. Talk to your Line Manager or immediate Supervisor immediately in the strictest confidence.
5. If you suspect it – report it again in the strictest confidence.