To Whom It May Concern

Re: Joint Operations UK LLP – Data Protection Information

Thank you for your recent enquiry in relation to the Data Protection provision that has been applied by Joint Operations UK LLP (the Company) in respect of the General Regulation of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) and then latterly the Data Protection Act 2018.

The Company recognises the importance of data protection as a principle in terms of the customers, suppliers, clients, consultants, engagers and all third parties who it trades with either directly or indirectly. This document and the schedules annexed hereto summarises the need for a company-wise programme (the Programme) which allocates resources and sets out the culture of the Company in dealing with the updated requirements of the data protection legislation as well proving the key information to evidence the ongoing steps that the Company has taken to ensure compliance and be able to evidence the same.

Issues concerning data protection under the GDPR

An immense volume of personal data continues to proliferate and flow daily around the UK and between the UK and other countries in the world. Some of this personal data needs to be accessible beyond the UK's borders.

Information, including personal data, is a valuable Company asset. Hard facts and figures are essential to making decisions. Information assets must be used effectively to meet business goals and the “Big Data” revolution, in particular, gives businesses great opportunities to exploit the information they hold for commercial advantage. A failure by the Company to hit the right balance between risk and opportunity in its use of data could have serious consequences for business in the future.

Personal data is defined broadly and comprises data relating to any living individual who can be identified from that data. Personal data and includes:

- Names.
- Addresses.
- Social security numbers.
- Telephone numbers.
- Health information of, for example, customers and employees.

There are many potential ramifications of failure to comply with the GDPR, including:

- Prosecution of or regulatory enforcement action against the Company, resulting in substantial penalties in European Economic Area (EEA) jurisdictions, including the UK, of up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is the greater).
- Adverse publicity, potentially leading to reputational damage and lost customer trust.
- Missed opportunities and wasted resources.
- A variety of sanctions in different jurisdictions.
- Increased scrutiny from data protection authorities whose confidence and powers are increasing substantially under the GDPR.
- Civil liability or punitive damages for employment-related breaches.

- Criminal liability for directors and senior managers resulting in imprisonment and substantial penalties.
- Critical system delays and failures.
- Orders issued by the Information Commissioner's Office in the UK, and data protection authorities in other key markets, that seriously impact business. Investigative powers include a power to carry out audits, as well as to require information to be provided, and to obtain access to premises.
- Business continuity issues.
- Becoming embroiled in litigation and its attendant time, effort and expense.

The aim of the GDPR is to ensure good information handling practice. For example, identity theft, stolen credit cards and failure to comply with privacy policies may result in fraud, theft and deception. Abuse of health data, financial data or children's data can have an adverse impact on insurance, credit, jobs or parental control.

An individual has a fundamental right in the UK and across the EEA to have their personal data protected and their personal data may only be processed (that is, obtained, recorded, held, used or disclosed) under certain circumstances. This has a wide impact on Company business.

The Programme

A well-constructed and comprehensive Company-wide programme can provide a solution to these various competing interests and represents an effective risk management tool. It is essential for compliance and to inform employees, customers, vendors, business partners, regulators and the courts of the Company's commitment to data protection.

Board's duty to know about and oversee the Programme

The Board has a duty to know about the content and operation of the Programme, and to oversee its implementation and effectiveness appropriately. The GDPR's new accountability principle requires data controllers to be able to demonstrate compliance with the GDPR by showing the supervisory authority (the Information Commissioner's Office in the UK) and individuals how the data controller complies, on an ongoing basis, through evidence of:

- Internal policies and processes that comply with the GDPR's requirements.
- The implementation of the policies and processes into the organisation's activities.
- Effective internal compliance measures.
- External controls.
- Failure to comply with the accountability principle may result in the maximum fines of up to €20 million or 4% of total worldwide annual group turnover.
- Implementing the Programme

Data protection officer (DPO)

Unlike certain types of organisation, it is not mandatory for the Company to appoint a data protection officer (DPO) under the GDPR.

However, taking into account the complexity of and risks associated with the GDPR, we should consider carefully whether we should appoint a DPO / Data Protection Manager in any case to report to the Board and provide the knowledge, expertise, day-to-day commitment and independence to properly advise the Company of its duties and conduct compliance activities in relation to the GDPR.

Organisational culture and chain of command

The Company must display an organisational culture that encourages compliance and provides staff with the clear guidance and tools they need to achieve it. It also requires that corporate leaders behave appropriately or are held accountable by the Board.

A co-ordinated chain of command will need to be developed, together with written reporting procedures, authority levels and protocols, including seeking and complying with legal advice.

The Company has already enacted the establishment of a working group, drawing on stakeholders from across the business, to take responsibility for the day-to-day management of the Programme.

Standards and procedures

The privacy policies are a key element of the Programme. Amendments are likely to be needed to the existing policy / policies.

Separate policies may be appropriate where the Company collects different types of personal data for different purposes, such as marketing and recruitment. In each case, the policy needs to be accessible at every relevant personal data collection point, for example:

- Emails.
- Call-centre conversations.
- Online account and job application forms.
- Business acceptance procedures.

In particular, the Company will need to carefully review existing procedures in relation to obtaining individual's consent as a legal basis for processing personal data. For example, it will need to ensure that any consent obtained indicates affirmative agreement from the individual (opt in) (for example, ticking a blank box). Mere acquiescence (for example, failing to un-tick a pre-ticked box) does not constitute valid consent under the GDPR. Furthermore, the Company must demonstrate that this explicit consent has been obtained, ensure that an individual can easily withdraw their consent at any time.

The Company must also be in a position at all times to respond quickly to any data subject's request (such as for a copy of all of the personal data held or to erase all such personal data). This is likely to require substantial modifications to the Company's technological infrastructure and its organisational processes.

Other channels may be needed in certain circumstances, for example, the staff handbook / standalone policies regarding personal data collected from employee monitoring.

A written and comprehensive information security programme is needed to protect the security, confidentiality and integrity of personal data held. It should set out action plans for security breach, disaster recovery and data restoration.

The Company should develop appropriate contractual strategies and have access to appropriate templates as a risk management tool.

Under the GDPR, the Company will also be required to implement "privacy by design" (for example, when creating new products, services or other data processing activities) and "privacy by default" (for example, data minimisation). It must also carry out "privacy impact assessments" before carrying any processing that uses new technologies (and taking into account the nature, scope, context and purposes of the processing) that is likely to result in a high risk to data subjects, takes place.

The GDPR also requires businesses to notify the supervisory authority of all data breaches without undue delay and where feasible within 72 hours. The Company will therefore need to look carefully at its data breach response plans and procedures.

The above represents only a short synopsis of the requirements under the GDPR. There are many more that are not included in this note for the sake of brevity. Getting prepared for compliance with all of the compliance requirements will need considerable planning across the Company.

Adequate resources

Financial, technological and human resources should be sufficient to reasonably prevent and detect non-compliance and promote compliance with the GDPR.

Training and enforcement

Effective compliance training programmes are required for personnel at all levels, including directors, heads of departments and key Company service providers. Bearing in mind the above factors, a formally documented training programme with employee evaluation and attendance certification should be put in place as soon as possible.

Serious misconduct should be addressed with appropriate disciplinary action, regardless of seniority. An anonymous whistle-blowing mechanism should be considered, but legal advice should be sought before implementation in the UK and any other countries in which the Company carries on business.

Regular reviews

From time to time, the Programme should be reviewed and updated in the light of new laws and business activities and changes to cross-border data flows.

Ensuring Appropriate Provision

The Company has identified the following key themes in terms of data protection and has enacted policies and procedures designed to address the material risks which stem from these themes. The headings below are designed to confirm the Company's position on these themes as well as to draw the results of the implementation Programme together from the separate policies into the bundle of documents attached.

a) Statement of Information and Governance

Full name of legal entity:	Joint Operations (UK) LLP
Name or title of data privacy manager:	Richard Forster
Email address:	richard@jointoperations.co.uk
Registered address:	21 Broadwalk Pinner Road, North Harrow, Middlesex, HA2 6ED
Telephone number:	01793 575050
Our Website:	https://jointoperations.co.uk/

The Company has taken the decision to become ISO9001 Quality System regulated and a copy of the certification and scope is provided in the bundle.

b) Internal Data Records

The Company has tracked the data which it holds via a Record of Processing Activities. This is designed to data map the information held by the Company to perform its services.

The Company has also produced a Data Retention Policy which sets out the terms upon which the data of the Company will be held and / or destroyed.

Whilst the Company has not yet needed to engage in this process, it has created a Privacy Impact Assessment tool. This will be completed should there be a need to examine the impact of a new technology or security measure.

c) External Statements

Those who trade with the Company will be able to view the Privacy Notice which confirms the data to be collected and the reasons for its collection.

The Company has undertaken a review of its supplier and customer contracts and will ensure that all of the information provided or acquired via a data sharing agreement will contain a provision which is broadly aligned with the data protection addendum. This is to ensure that the necessary written statements are produced for each data sharing arrangement.

d) Management of Employees (relevant to data protection only)

Staff will be managed via the Data Protection Policy and will be suitably trained on its requirements in terms of their own and the businesses responsibility toward data protection.

The data of employees and candidates will be covered by the Staff and candidates Privacy Notices as well.

The statements that staff can make to external third parties would be covered by the Media Policy. This would be statements that can be made over social media or to the media in general.

Where staff provide services from their home address this would be covered by the Homeworking Policy.

e) Security, Resilience and Access Controls

Security and resilience is a broad concept but the Company is dedicated to ensuring that there are sufficient controls in place to govern use of data. The below policies would be in addition to the above 'staff management' policies as well.

The Disaster Recovery Policy sets out the contingencies for what would happen if a catastrophic business event took place.

Security around staff devices is covered by the Bring Your Own Device Policy and then the IT and Communications Policy covers the terms of use and then enforcement action should this be breached.

Generalised protections and security measures are covered by the data protection policy and privacy notice and data retention policy.

Summary

A suite of documents is available on request to evidence the above and to satisfy the obligations of the Company towards Accountability and Compliance.

Kind regards,

Richard

Richard Forster
Data Protection Manager
Joint Operations (UK) LLP