United Kingdom – Data Privacy

The United Kingdom ("UK"), as a member of the European Union ("EU"), was required to implement the EU Data Protection Directive 95/46/EC (the "Directive") into its national legislation. The Directive was implemented in the UK in March 2000 when the Data Protection Act 1998 (the "Act") came into force and all personal data became subject to the Act by October 24, 2007. The Office of the Information Commissioner (the "Information Commissioner") enforces the Act. In June 2005, the Information Commissioner published the Employment Practices Data Protection Code to assist employers in understanding and complying with the Act.

Collection and Processing of Personal Data	
Compliance Alternatives	"Processing" of personal data has a very wide definition and essentially covers most operations relating to the data, including its collection, storage and transfer. Processing is allowed where: 1) the employee consents; 2) it is necessary for the performance of a contract to which the employee is a party; 3) it is necessary to comply with a legal obligation to which the employer is subject; 4) it is necessary in order to protect the vital interests of the employee; 5) it is necessary for the administration of justice, the functions under any enactment, the Crown, the government, or public functions in the public interest; or 6) it is necessary for legitimate interests pursued by the employer, or third party recipients, unless it prejudices the rights and freedoms or legitimate interests of the employee. These conditions are subject always to the processing being "fair and lawful". With respect to the collection and processing of sensitive data (e.g., racial or ethnic origin, political opinions, party affiliation, and religion), additional requirements apply.
Disclosure/ Registration	An employer, as a "data controller", is required to notify the Information Commissioner and register databases containing employees' personal data. Details of the employer are entered into the Register of Data Controllers and made publicly available. The notification must include descriptions of the data, such as the types of data to be collected, the employees about whom the data will be held and the purposes for which the data will be processed. The Information Commissioner must be notified of any changes or amendments to any entry in the Register of Data Controllers.
Other Requirements	Personal data must: 1) be obtained for specified and lawful purposes; 2) not be processed in a manner incompatible with such purposes; 3) be adequate, relevant and not excessive in relation to the purpose for which they are processed; 4) not be kept for longer than is necessary for the purpose; and 4) be kept accurate and up-to-date. Appropriate technical and organizational measures must be taken against unauthorized or unlawful processing of, accidental loss or destruction of, or damage to, personal data.
Transfer of Personal Data	
Compliance Alternatives	The cross-border transfer of personal data outside of the European Economic Area ("EEA") is prohibited unless that country ensures an "adequate level of protection" in relation to the processing of personal data. Derogations to this prohibition include where: 1) the employee consents to the transfer; 2) it is necessary for the employment contract; 3) it is necessary for the performance of a contract between the employer and a third party that is in the interest of the employee; 4) it is necessary on substantial public interest grounds; 5) it is necessary in connection with legal proceedings; 6) it is necessary to protect the vital interests of the employee; or 7) the data is from a public register. To the extent that countries outside the EEA provide an adequate level of protection in relation to the processing of personal data, transfer of data is permitted. The UK has approved three sets of standard contractual clauses for cross-border data transfers and is a keen advocate of Binding Corporate Rules, pursuant to which employee consent is not required. Non-standard contracts and codes of conduct are also acceptable provided a sufficient finding of adequacy has been made in relation to the safeguards afforded to the personal data. For the transfer of data to the US, the UK will view compliance with the US/EU Safe Harbor principles as compliance with the cross-border transfer law in the UK.
Other Requirements	If data will be subject to transfers outside the EEA, such information must be reflected in the notification to the Information Commissioner.