Denmark – Data Privacy

The Danish Constitution of 1953 contains provisions relating to privacy and data protection. Denmark, 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 Denmark pursuant to the Act on Processing of Personal Data (the "Act"), which became effective in 2000. An independent agency, the Data Protection Agency ("DPA") enforces the Act.

Collection and Processing of Personal Data	
Compliance Alternatives	In general, personal data may be processed in circumstances including where: 1) the employee has given his or her explicit consent; 2) processing is necessary (a) for the performance of a contract to which the employee is a party (an employment relationship is a de facto contract) or (b) to take steps at the employee's request prior to entering into a contract; 3) processing is necessary for compliance with a legal obligation to which the employer is subject, 4) processing is necessary in order to protect the vital interests of the employee; 5) processing is necessary for the performance of a task carried out in the public interest; 6) processing is necessary for the performance of a task carried out in the exercise of official authority vested in the employer or in a third party to whom the data are disclosed; or 7) processing is necessary for the purposes of the legitimate interests pursued by the employer or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the employee. Absent an exemption (e.g., the employee's explicit consent), sensitive data such as racial or ethnic origin, political opinions, party affiliation, and religion may, however, not be processed.
Disclosure/ Registration	Generally, the DPA must be notified prior to the processing of personal data. However, several exemptions apply to this notification requirement, e.g. the employers processing of non-sensitive personal data regarding employees does not require notification to the DPA. In situations where a notification to the DPA is required, the DPA will be required to record the data processing activities in a register accessible by the general public.
Other Requirements	The employer must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions set out in the Act. An employee may withdraw his or her consent to the processing of data relating to him or her. The employer must, at the request of the employee, rectify, erase, or block data which turns out to be inaccurate or misleading or is in any other way processed in violation of law or regulations. Upon request from the employee, the employer is obliged to inform the employee whether or not data relating to the employee are being processed, and if data is being processed, the employer shall notify the employee about 1) the data that are being processed, 2) the purposes of the processing, 3) the categories of recipients of the data, and 4) any available information as to the source of such data.

Transfer of Personal Data	
Compliance Alternatives	The transfer of data to a country outside the EU/EEA may take place only if the third country in question ensures an adequate level of data protection. Additionally, transfer of data to a third country may take place if: 1) the employee has given his explicit consent to the transfer; 2) the transfer is necessary (a) for the performance of a contract between the employee and the employer or (b) to take steps at the employee's request prior to entering into a contract; 3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the employee between the employer and a third party; 4) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; 5) the transfer is necessary in order to protect the vital interests of the employee; 6) the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests; 7) the transfer is necessary for the prevention, investigation, and prosecution of criminal offenses and the execution of sentences or the protection of persons charged, witnesses or any other persons in criminal proceedings; or 8) the transfer is necessary to safeguard public or national security. If the data includes sensitive data (or is carried out for certain specific purposes such as warning third parties against entering into an employment relationship with the employee) and the legal basis for the transfer is number 2), 3) or 4), prior approval of the transfer must be obtained from the DPA. The DPA may authorize a transfer of personal data to a third country with an inadequate level of protection if an employer provides adequate safeguards with respect to the protection of the rights of the employee. The DPA may require the fulfillment of additional conditions for such a transfer. Use of standard contractual clauses is advised to facilitate DPA authorization for data transfer. The EU commission has prepared a model contract that can be used. In addition to the standard contractual clauses, it is also possible to provide adequate guarantees by using so-called binding corporate rules (BCR). These are rules enacted for groups with companies in multiple countries. The rules must be binding for all units and companies in the group. Furthermore, personal data may be transferred to US companies participating in the Safe Harbor program, as such companies due to the Safe Harbor data processing obligations are considered to ensure an adequate level of data protection.
Other Requirements	None applicable.

