Employee Data Privacy – Singapore

Security Requirements

What security obligations are imposed on data controllers and data processors?

Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, prevent alteration, corruption or access by unauthorized third parties.

Appropriate technical and organizational measures should be implemented to ensure a level of security appropriate to the risk.

Under the Protection Obligation in Singapore's Personal Data Protection Act 2012 (PDPA, Part VI, Sec. 24), employers are required to make reasonable "security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to personal data in its possession or under its control." Under the Advisory Guidelines on Key Concepts in the PDPA (July 2017, The Protection Obligation) companies are advised to:

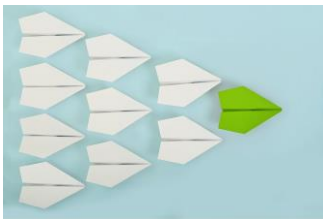
- design and organize security around data protection to fit the nature of the data and the risk of harm that may result from a security breach;
- select "reliable and well-trained" employees to be in charge of information security;
- implement strong policies and procedures to ensure security appropriate to the personal data's sensitivity; and,
- prepare for the potential for security breaches and, respond to any breaches promptly and effectively.

Employers may also want to undergo risk assessment exercises to assess whether current information security practices are adequate, based on the: size of the organization, the

amount/type of personal data, the individuals who have access, and whether the data will be held/used by a third party.

Security arrangements may include administrative, technical and/or physical measures. Administrative measures can include confidentiality obligations, policies, regular trainings and limiting the data that is held. Physical measures can include clearly marking confidential documents, storing confidential personal employee data in locked cabinets, restricting employee access, using privacy filters on laptops, proper disposal, etc. Technical measures can include securing computer networks, adopting access controls, encrypting data, regularly updating computer and IT equipment, etc.

HR Best Practices:



The majority of enforcement cases relating to the PDPA involve breaches of the Protection Obligation. Employers in Singapore should take all reasonable steps to protect the personal data of employees and applicants, including undergoing risk assessments to see where there may be gaps. Ensure contracts with service providers detail the security and confidentiality measures that will be implemented. In addition, regularly train employees who may have access to personal information to ensure that they are following all technical and organizational security measures that have been put in place.

Last updated March 2023.