Employee Data Privacy – Malaysia

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. Employers in Malaysia should follow the general security standards set in the Personal Data Protection Act 2010. Data processors are expected to take practical steps to protect personal data from loss, misuse, modification, unauthorized/accidental access or disclosure/alteration/destruction.

When protecting employee and applicant data, consider the sensitivity of the information and the risk of harm to individuals if the data were compromised. Additional considerations should include: the physical place data is stored; the security measures incorporated into equipment; the measures taken to ensure the reliability, integrity and competence of individuals who have access to the data; and, the measures taken to securely transfer data.

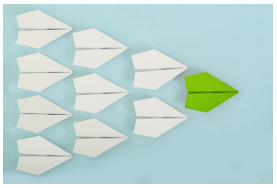
When using third parties to process data, ensure they provide sufficient guarantees relating to technical and organizational security standards; and, take reasonable steps to comply with those standards.

In addition, the Personal Data Protection Standard 2015 sets additional guidelines for protecting electronically processed data, including:

- registering employees who process personal data;
- terminating access rights after an employee leaves the company or is no longer handling the data;
- limiting and controlling access to personal data systems;
- authenticating individuals authorized to access personal data through user IDs and passwords;

- taking physical measures to secure data by controlling who can access the data storage site;
- storing data in an area where it's protected from physical and natural threats, using video security (if necessary and/or security monitoring)
- updating systems including back-up systems with anti-virus software and safeguarding from malware;
- limiting physical data transfers unless there is written consent from the individual in charge of managing the data;
- recording any data transfers;
- maintaining a record of data access (and making it available to the data protection Commissioner if requested);
- ensuring employees protect the confidentiality of the personal information; and,
- using contractual agreement with third parties who process or access data.

Similar data security measures are expected for data that is processed non-electronically. In cases where data is stored physically, employers should use registration books/systems to track access, destroy outdated data, and take additional physical security measures (i.e. lock the files and protect keys/access to those files).



HR Best Practices:

Make sure to destroy both physical and electronic data once it is no longer needed. 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 April 2023.