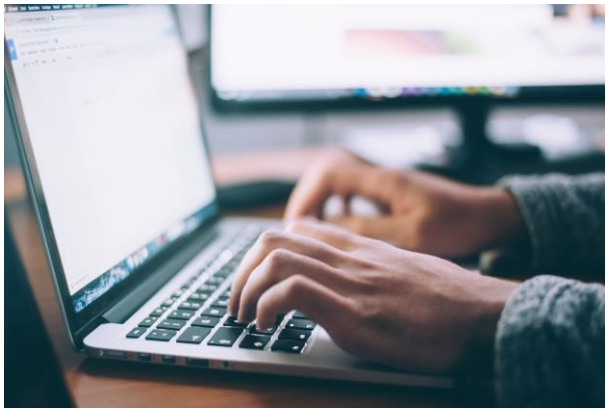
Employee Data Privacy – Hong Kong

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.



Security is one of the six principles of Hong Kong's Personal Data (Privacy) Ordinance (Cap. 486). Employers, and other data users, must take reasonable steps to safeguard personal data and protect it from unauthorized/accidental access, processing, deletion loss and use. Employers should consider the most practical ways to protect the data given the: type of data being collected (and the potential for harm if not adequately protected); physical location where the data is housed; security measures incorporated into equipment; measures to ensure the integrity, prudence and competence of individuals who have access to personal data; and, measures to ensure secure transmission.

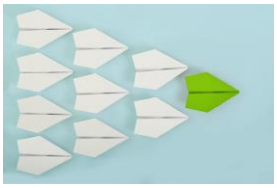
When using third-party data processors inside or outside Hong Kong, employers must adopt contractual or other means to protect the personal information.

Appropriate technical and organizational measures are recommended to ensure a level of security appropriate to the risk, including:

- personnel related measures, such as training staff to ensure they understand and are following personal data privacy policies,

having staff sign confidentiality agreements, regularly updating policy manuals, etc.;

- controlling who and how personal data is accessed. Computer protection measures can include regularly updating security features, password protection, dedicated access terminals, automated audit trails, prohibiting unauthorized copies, etc. Third-party data processing measures must include contractual or other means to ensure security;
- destroying data that is no longer needed via secure means; and,
- measures to protect personal employee data that is transferred via the internet, such as software encryption.



HR Best Practices:

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 February 2023.