

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.



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.

HR Best Practices: Ensure contracts with service providers detail the security and confidentiality

Last updated August 2018.

DISCLAIMER: The information contained in this form is for general information purposes only and is not intended to be a source for legal advice and should not be relied upon as such. This information is not intended to create, and the receipt of it by the reader does not constitute, an attorney-client relationship. Organizations or individuals receiving this document should always seek the advice of competent counsel in their home jurisdiction. Laws may change and PeopleDoc cannot guarantee that all the information in this form is current or correct. PEOPLEDOC DOES NOT GIVE ANY EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY, OR COMPLETENESS OF THIS INFORMATION. TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, NEITHER PEOPLEDOC, NOR ITS AGENTS, OFFICERS, EMPLOYEES, OR AFFILIATES, ARE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE OR PROFITS, OR BUSINESS INTERRUPTION), EVEN IF PEOPLEDOC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT, ARISING IN ANY WAY OUT OF THE USE OF OR INABILITY TO USE THIS INFORMATION. The content of this document is proprietary and confidential information of PeopleDoc. It may not be distributed to any third party without the written consent of PeopleDoc. © 2018 PeopleDoc Inc. Do not reproduce without the written permission of PeopleDoc Inc.

PeopleDoc HR Compliance Assist

HR Compliance Assist helps PeopleDoc clients proactively and effectively manage compliance of their HR files and employees' data with foreign laws and regulations. Led by PeopleDoc's Chief Compliance Officer, the HR Compliance Assist team relies on a network of internal and external lawyers to provide clients with best practices and recommendations on topics such as HR document retention, employee data privacy, electronic signature and electronic archiving. HR Compliance Assist also provides local compliance monitoring and alert services in select countries where PeopleDoc's customers have employees. HR Compliance Assist is a service available to PeopleDoc customers.

PeopleDoc is on a mission to make the difficult job of HR easier. The PeopleDoc HR Service Delivery platform helps HR teams more easily answer employee requests on demand, automate employee processes, and manage compliance across multiple locations. PeopleDoc cloud solutions include case management, process automation and employee file management.

100% software as a service, PeopleDoc solutions integrate with existing HR systems, can be implemented in 8-12 weeks, and are designed for agile ongoing use by HR teams serving diverse workforces. More information is available at www.people-doc.com.



HR Compliance Assist

www.hrcomplianceassist.com - hrcomplianceassist@people-doc.com