



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,

UKG HR COMPLIANCE ASSIST

- 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.

DISCLAIMER: The information contained in this document is for general information purposes only and is not intended to be a source for legal, tax, or any other professional 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. All legal or tax questions or concerns should be directed to your legal counsel or tax consultant. Laws and regulations may change and UKG Inc. ("UKG") cannot guarantee that all the information in this document is accurate, current or complete. UKG MAKES NO REPRESENTATION OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE DOCUMENT OR THE INFORMATION OR CONTENT CONTAINED HEREIN AND SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES INCLUDING BUT NOT LIMITED TO ANY EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY, OR COMPLETENESS OF THIS INFORMATION. TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, NEITHER UKG, NOR ITS AGENTS, OFFICERS, EMPLOYEES, SUBSIDIARIES, 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 THE UKG 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. This document and the content are proprietary and confidential information of UKG. No part of this document or its content may be reproduced in any form, or by any means, or distributed to any third party without the prior written consent of UKG © 2023 UKG Inc. All rights reserved.