



# Employee Data Privacy – China

## 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.



China's Personal Information Protection Law provides that data controllers (such as employers) adopt necessary measures

to ensure that personal information processing complies with the provisions of Chinese laws and regulations and prevents unauthorized access or personal information leakage, tampering, and loss of personal information, such as:

- formulating internal management systems and operating procedures;
- implementing classified management of personal information;

- adopting appropriate technical security measures, such as encryption and de-identification;
- reasonably determining operational limits for personal information processing and regularly conducting employee security education and training;
- formulating and organizing the implementation of information security incident response plans; and,
- other measures provided by Chinese laws and regulations.

Under the Civil Code, information processors must: implement technical and other necessary measures to ensure the security of personal information that is collected and stored; and, prevent the information from being leaked, tampered with, or lost. If personal information has been or is likely to be leaked, tampered with, or lost, the information processor must take remedial measures in a timely manner, notify natural persons who are impacted in accordance with the regulations, and report the incident to the relevant competent authorities.



### HR Best Practices:

Employers should take necessary measures to ensure the security of personal information, prevent leakage or loss of personal information and take remedial measures immediately when leakage or loss of information occurs.

Last updated September 2022.

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 © 2022 UKG Inc. All rights reserved.