



Employee Data Privacy – South Korea

Fines and Penalties

What are the penalties for noncompliance with any applicable data protection laws?

Noncompliance with Data Privacy Laws and Data breaches may lead to sanctions, fines, and penalties. The amounts are usually calculated according to the risk to which personal rights were exposed and the preventive measures taken by the data controllers, processors and sub-processors in relation to their respective role in the chain of personal data processing.

South Korea has a range of penalties including criminal fines as high as 100 million won or 10 years' imprisonment. Penalties, such as criminal fines of up to 50 million won or 5 years' imprisonment, can be incurred for improperly providing information to a third party without the consent of the data subject; using personal information for marketing or an unfair purpose, or purposeful damage/destruction/forgery, etc.

In addition, in the case of loss, theft, leakage or falsification of resident registration numbers, a penalty of up to 500 million won can be imposed on the data handler. In order to avoid this, the data handler must prove that it has taken all necessary data security measures as prescribed under the PIPA.

Smaller penalties and fines can be incurred for offences such as mishandling visual data; obtaining information or consent through fraud/unjust means; receiving information knowingly for profit or unfair purpose; divulging confidential information or using information for purposes other than the initial one.



There is no specific penalty imposed for failure to make or maintain an entry on the register. However, if failing to make/maintain an entry on the register is deemed to fall under any of the aforementioned violations, the associated penalty could be imposed.



HR Best Practices:

Before processing personal data, make sure to be in-line with the security measures

necessary, as required under PIPA, to ensure data security within your organization. In addition, ensure all data processors have data breach response plans in place.

Last updated February 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.