

Employee Data Privacy – South Korea

Employee Consent

Do I have to obtain employees' consent in order to collect their personal data?

The processing of any personal data may impose obligations to the individuals the data is related to, the data subjects. Some jurisdictions only recognize processing personal data as lawful if the data subject has provided express consent. Other jurisdictions require a legal obligation to process the data and may not require consent. The processing of HR personal data has raised questions and court decisions in a few countries, and interpretations may vary based on data privacy and labor law requirements. The concept of employee consent has been increasingly criticized because there is doubt as to whether consent can be given freely in the subordinate employee/employer relationship.

Consent is one of the core rights of data subjects under South Korea's Personal Information Protection Act (PIPA), and individuals have the right to choose whether to consent and elect the scope of the consent relating to the processing of their personal information.

Employers are allowed to collect personal information without consent in the following cases:

- where allowed by law or where it's inevitable in order to observe legal obligations (such as tax obligations);
- where it's inevitable so public institutions can perform their official duties;
- where it's necessary in order to fulfill a contractual obligation (such as an employee contract);
- where it's necessary for the justifiable and reasonable interests of the employer (or other personal information controller) and those interests are explicitly superior to the needs of the employee (the data subject); and,
- when it's necessary to protect from impending danger, the life, body or economic profits of the data subject and the data subject is not available.



Sensitive Personal Information

In principle, employers are not allowed to process sensitive information, including: ideology, beliefs, admission to/withdrawal from trade/political parties, political beliefs, health, sexual life or, other personal information that is likely to threaten the privacy of the employee (or any

UKG HR COMPLIANCE ASSIST

other data subject). However, sensitive information may be processed in cases where:

- data subjects give express informed consent (separate from the consent above) to the processing of sensitive information; or
- the processing of sensitive information is specifically permitted by a law or regulation.



Employee Health Information: Using employee health information for purposes other than maintaining employee health

protection is generally prohibited. That said, in exceptional cases, when processing employee health information is essential, it may be allowed with the employee's consent.

In cases where processing medical files is permitted in the context of HR, if a health exam is conducted to determine whether a job applicant can perform the necessary duties for a role, only the minimum amount of health information may be collected and consent must be obtained. In addition, the use of health information obtained through an employee health exam is allowed without separate consent when the exam is conducted in accordance with statutes maintaining employee health protection (Note that many employers still obtain consent).

Resident Registration Numbers: Processing resident registration numbers is also limited and can only be processed for certain purposes. In the context of HR, examples of permitted purposes include payment of wages and for year-end tax settlement (Act on the Collection, etc. of

Premiums for Employment Insurance and Industrial Accident Compensation Insurance; National Pension Act; National Health Insurance Act to deal with industrial accident compensation insurance, health insurance, employment insurance and national pensions; and, the Income Tax Act).

Informing Employees

When obtaining consent or modifying the purpose of collecting data, employers should inform employees of the (PIPA, Arts. 15(2) and 17(2)):

- purpose of the collection and use of the data;
- details of the personal information that will be collected;
- the period of retention and use;
- the fact that they are entitled to deny consent and, in addition, inform employees of any disadvantage that may stem from the denial of consent.

Consent can be obtained via writing (electronic, fax or paper), telephone, email, the internet or similar manner. Where consent is used, each item that would require consent should be separated so that an individual is able to choose which items to consent to. The mere act of informing individuals of the personal data collection will not suffice. The individuals must be advised of the items above and must provide their explicit consent to the collection of personal information.

Under the PIPA, employers are not required to obtain the consent of employees when outsourcing the processing of personal

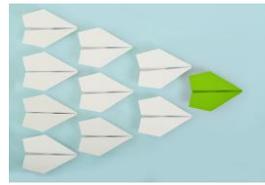
UKG HR COMPLIANCE ASSIST

information. When providing personal employee data to a third party, employees must be informed of:

- the recipient of the personal information;
- what the recipient will use the personal information for (the purpose);
- the particulars of the personal information that is being provided;
- the period the personal information will be used and retained; and,
- that they (as the employees) are entitled to deny consent, and any disadvantage which may result from their denial.

Consent is not required if the processing of personal information is outsourced to a foreign

entity, but employers must include information on the specific tasks to be outsourced and the name(s) of the outsourced processor(s) in their privacy policy, so that such information is readily available to employees. Employees must be notified when data is being transferred out of South Korea and/or when personal information is being collected from third parties.



HR Best Practices:

Even if consent is not required, employees and job applicants should be properly informed prior to data collection. Although consent in writing is not required, as a best practice, obtain employee consent in writing in case it is ever questioned in court.

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.