Employee Data Privacy – South Korea

Fines and Penalties

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

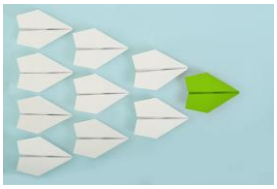
Noncompliance with Data Privacy Laws and Data breaches may lead to sanctions, fines, and penalties. The amounts are usually calculated according to the risk to which personal rights were exposed and the preventive measures taken by the data controllers, processors and sub-processors in relation to their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