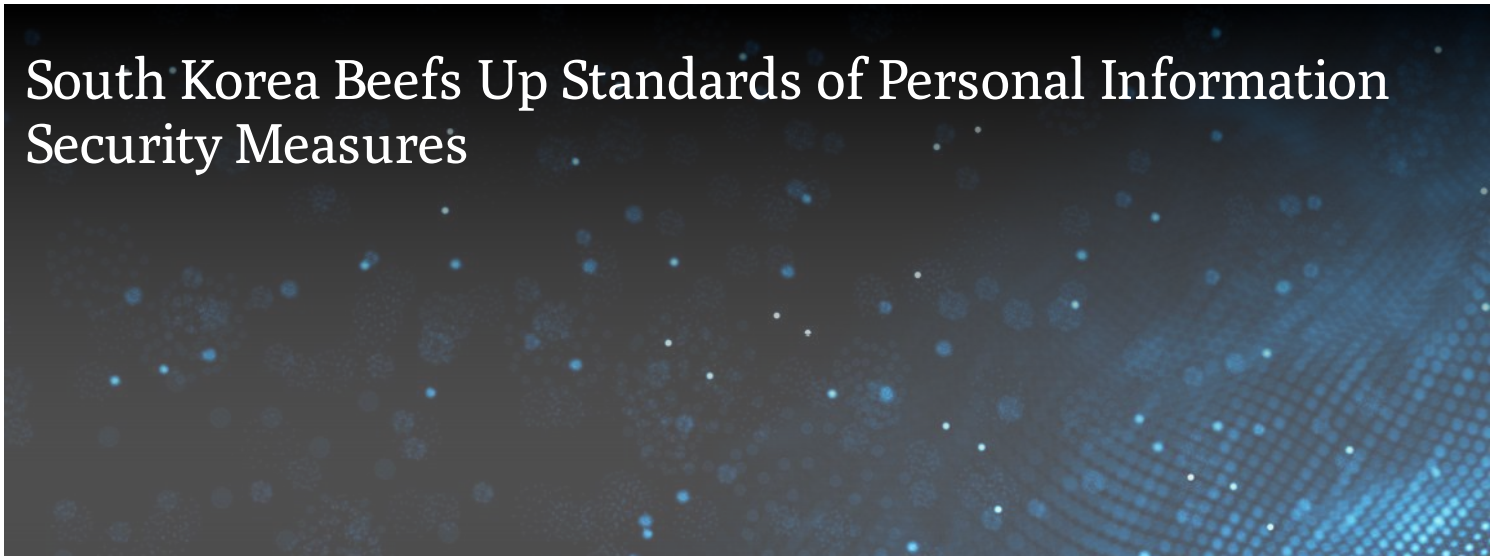
WINSTON & STRAWN LLP

BLOG

South Korea Beefs Up Standards of Personal Information Security Measures



MAY 6, 2015

In response to recent major data breach incidents involving South Korea's three largest credit card companies, the South Korean Ministry of Government Administration and Home Affairs issued new amendments to the existing Standards of Personal Security Measures, which came into force on December 30, 2014. The amendments are intended to address gaps in the Standards given the increasing propensity of data handlers to outsource data processing to third party providers and the increasing use in the workplace of mobile devices to process personal information. We set out below a summary of the key features and developments.

Outsourced Providers: The amendments place stricter obligations on data handlers to actively monitor and manage the activities of their third party service providers. In particular, data handlers must disclose full details of their outsourcing management policy and ensure that outsourced providers comply with all relevant data protection legislation. The key element is regular, engaged, and pro-active supervision of such providers, otherwise data handlers may be subject to increasingly severe penalties.

Security Requirements for Mobile Devices: Mobile devices are now expressly included in the Standards as being personal information processing systems and, accordingly, must have adequate security functions to prevent and control the leaking of personal information to unauthorized recipients. In the case of particular identification data (i.e. sensitive data), this means that mobile devices must have a specific encryption function.

Ongoing Periodic Checks: Under the amended Standards, data handlers that process particular identification data must conduct an inspection at least every six months of access records or logs. They must also put in place adequate security measures to monitor and control the use of portable storage devices such as USB and other external drives. In addition, they must undertake a separate annual inspection to assess security measures and the risk of such data being leaked, tampered with, damaged, or destroyed.

Destruction of Personal Information: The amendments to the Standards set out new and enhanced requirements for the destruction of personal data held by data handlers, which are aimed at ensuring that the data cannot be copied or restored, whether it is in hard-copy form or electronic form, especially in situations where some, but not all, personal information are being destroyed.

TIP: The amendments to the Standards are a direct response to recent high-profile incidents. This is an area that is being monitored closely by regulators in South Korea and there are rumors of other new laws and

regulations. Data handlers should ensure that they have in place adequate procedures in relation to outsourced providers, check that any mobile devices used by their employees have the relevant security functions, and make arrangements for the required periodic access and risk inspections.

2 Min Read

Related Locations

Chicago

Related Topics

Asia Privacy

Data Breach

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.

© 2025 Winston & Strawn LLP.