NEWSLETTER

June 2021

Data Privacy & Cybersecurity Group

CONTACT

Kwang Bae PARK

T: +82.2.772.4343
E: kwangbae.park@leeko.com

Hwan Kyoung KO

T: +82.2.2191.3057
E: hwankyoung.ko@leeko.com

Sunghee CHAE

T: +82.2.6386.6622
E: sunghee.chae@leeko.com

Changes to CISO Designation Rules and Public Disclosure Requirement for Information Security

Certain amendments to the Act on Promotion of Information and Communications Network Utilization and Information Protection (**Network Act**) and the Act on the Promotion of Information Security Industry (**Information Security Industry Act**) were promulgated on June 8, 2021 and are scheduled to go into effect on December 9, 2021. These amendments contain several major changes to the chief information security officer (**CISO**) designation rules under the Network Act, and the public disclosure requirements for information security matters under the Information Security Industry Act. Below, we provide an overview of the changes made by the promulgated amendments.

1. Key Provisions of the Amendment to the Network Act

Under the current Network Act, an information and communications service provider (**ICSP**)* that meets certain criteria set forth in the Enforcement Decree of the Network Act must designate a CISO and report such designation to the Minister of Science and ICT (Article 45-3(1)). An ICSP based outside of Korea may also be subject to this designation and reporting obligation, in addition to other CISO-related requirements as described below.

* Typically, a company which provides services using the internet (e.g., a website or an application) is viewed as an ICSP.

In addition, CISOs of (i) ICSPs with total assets of KRW 5 trillion (approx. USD 4.5 billion) or more as of the end of the previous business year, or (ii) ICSPs that are required to obtain the Information Security Management System (**ISMS**) certification under Network Act and have total assets of KRW 500 billion (approx. USD 4.5 million) or greater (collectively with (i), the "Companies Subject to the CISO Restriction") may not simultaneously perform other tasks within the company aside from those tasks which must be performed by a CISO as prescribed by law. As a result, the CISOs of the Companies Subject to the CISO Restriction have not been able to hold the role of chief privacy officer (**CPO**) simultaneously, thus making it necessary for companies to appoint separate individuals to the positions of CISO

and CPO. These restrictions have led to practical difficulties on the part of such companies in handling matters relating to the company's data security.

Although the amended Network Act continues to prohibit CISOs of the Companies Subject to the CISO Restriction from simultaneously performing any tasks within the company which are unrelated to those which the CISO is legally required to perform, it now explicitly provides for a number of exceptions to this prohibition. Specifically, under the amended Network Act, a CISO would be allowed to simultaneously perform the "tasks of a data protection officer under the Personal Information Protection Act" and the "tasks of a CISO under the Electronic Financial Transactions Act," among others. These relaxed CISO rules are likely to relieve many companies of the burdens of having to separately appoint a CISO and CPO.

A. Relaxed CISO qualifications and reporting obligation for companies

(1) Under the current Network Act, ICSPs who are required to appoint a CISO must do so from the company's executive-level personnel, which has not always been easy for companies (especially smaller-sized businesses) in terms of managing their human resources and operating their organization. Once becoming effective, the amended Network Act will allow companies to choose their CISO from among officers and employees who meet the qualifications prescribed by the Network Act's Enforcement Decree, so the companies will have the option to designate a non-executive-level employee as their CISO. Indeed, the Ministry of Science and ICT (**MSIT**) is reportedly in the process of amending its Enforcement Decree at the moment so that companies other than the Companies Subject to the CISO Restriction may designate a department head-level employee as their CISO.

(2) The amended Network Act also relaxes the reporting requirement for companies that are required to designate a CISO thereunder. The current Network Act provides that any ICSP required to appoint a CISO has to report such designation to the MSIT once its CISO is appointed. However, under the amended Network Act, those ICSPs that do not meet the thresholds prescribed by Enforcement Decree in terms of their total assets and sales would be exempted from the reporting requirement. The detailed thresholds will also be set forth in the Enforcement Decree of the Network Act, which is currently being amended by the MSIT. The new exemption is intended to relieve the burden on smaller-sized companies from having to designate a CISO, and thus, the thresholds will effectively still require "medium-sized companies"** and large companies that typically handle greater amounts of data (and thus have a need for heightened information security) to report their CISO designation to the MSIT.

** "Medium-sized companies" as defined under Article 2(2) of the Framework Act on Small and Medium Enterprises and Article 8(2) of the Enforcement Decree of the same Act.

B. Additional penalty provisions for non-compliance with the CISO-related regulations

While the CISO-related regulations under the current Network Act (collectively, **CISO Regulations**) have been relaxed as a result of the amendments, the amended CISO Regulations, once they go into effect, would likely be enforced more strongly.

Under the current Network Act, an ICSP may be subject to an administrative fine of up to KRW 30 million for its failure to report the designation of a CISO. As for any other violation of the CISO Regulations, an ICSP may only be subject initially to a corrective order issued by the MSIT. Under the amended Network Act, an administrative fine may also be imposed on ICSPs that fail to comply both with the prohibition for a CISO to assume another position or the CISO's qualification requirements set forth in the amended Network Act.

Since the MSIT is likely to strengthen its enforcement of the CISO Regulations by exercising the additional enforcement power conferred by the new penalty provisions of the amended Network Act (e.g., conducting a compliance survey on the implementation of the CISO Regulations), ICSPs obligated to designate a CISO should make the necessary preparations to comply with the amended CISO Regulations before they go into effect on December 9, 2021.

2. Key Provisions of the Amendment to the Information Security Industry Act

Under the current Information Security Industry Act, companies may voluntarily choose to publicly disclose information regarding their current status of information security (e.g., status of investment in and human resources for information security, certification related to information security), but are not required to do so.

However, under the amended Information Security Industry Act, companies whose public disclosure of information security is deemed necessary based on specific criteria (to be prescribed by its Enforcement Decree) will be required to publicly disclose information regarding their current status of information security and may face an administrative fine (of up to KRW 10 million) for a failure to do so.

The detailed scope of "companies whose public disclosure of information security is deemed necessary," which will be defined based on criteria such as a company's line of business, annual revenue, and number of users, is expected to be announced by the MSIT by the end of this year as part of amendments to its Enforcement Decree.

The foregoing changes appear to reflect growing public sentiment which increasingly regards a company's information security levels as constituting an important part of such company's overall soundness and competitiveness. Should such public disclosure proliferate after the amended Information Security Industry Act goes into effect, the details of such disclosure may end up becoming an important consideration when assessing the information security levels of companies facing potential criminal, administrative, and/or civil liability due to the occurrence of information security incidents.

Therefore, once the amended Information Security Industry Act takes effect, companies subject to the public disclosure requirements may need to start monitoring and benchmarking the information security measures (e.g., level of investments therein, human resources devoted thereto, certifications obtained therefor) of other companies of similar size and business profile to check if they are undertaking comparable efforts for information security.

We hope the foregoing update is helpful. If you have any questions and/or require any assistance, please contact Lee & Ko's DPC (Data Privacy & Cybersecurity) team.

For more information pertaining to this newsletter, please contact the attorneys identified on the left.

More L&K Newsletters | COVID-19 Resource Center

Lee & Ko

Hanjin Building 63 Namdaemun-ro, Jung-gu Seoul 04532, Korea | Tel: +82-2-772-4000 | Fax: +82-2-772-4001/2 | www.leeko.com