LEGAL UPDATE

bkl

June 9, 2021

National Assembly passes partial amendments to IT Network Act, allowing designation of non-executive level employee to Office of Chief Information Security Officer, etc

On May 21, 2021, the Korean National Assembly passed partial amendments to the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the "**IT Network Act**"). The amendments were promulgated on June 8, 2021 in the official legislative gazette and will take effect 6 month after the promulgation.

The key amendments are as follows:

(1) SMEs may appoint non-executive level employees as Chief Information Security Officer ("**CISO**"). Although the specifics of the amendments are to be stipulated in the Presidential Decree to the IT Network Act, the Ministry of Science and ICT ("**MSICT**"), the regulatory authority with oversight over the IT Network Act, has indicated that manager-level employees ("부장급 직원") may be designated as CISO for those IT Service Providers (as explained below) meeting certain criteria.

(2) The types of offices that can be concurrently held by a CISO are expanded to include, among others, the Office of Chief Privacy Officer ("**CPO**").

(3) Appointing CISO who is not qualified and/or holding concurrent positions in violation of the IT Network Act will each be subject to an administrative fine of up to KRW 30 million (approx. USD 27,000).

1. Appointing Non-executive Level Employees to the Office of CISO

Under Article 45-3 (1) of the current IT Network Act, providers of information and communications services ("**IT Service Providers**")—which effectively include any service provider conducting business online—are

Tae Uk KANG
T 82.2.3404.0485
E taeuk.kang@bkl.co.kr

Susan Park
T 82.2.3404.0274
E susan.park@bkl.co.kr

Jong Yoon KIM
T 82.2.3404.1958
E jongyoon.kim@bkl.co.kr

required to appoint an executive-level CISO.

The amendments will allow IT Service Providers to designate employees meeting certain criteria required under the Presidential Decree, thereby eliminating the requirement for an "executive-level" appointment for the CISO position. The specific criteria under the Presidential Decree will become available at some point before the amendments take effect.

In this regard, MSICT has expressed its intent to allow appointing manager-level ("부장급") CISO for those IT Service Providers that are not subject to the following:

(1) The IT Service Provider's total assets amount to at least KRW 5 trillion (approx. USD 4.5 billion); or
(2) (a) the IT Service Provider's total assets amount to at least KRW 500 billion (approx. USD 450 million) and (b) the IT Service Provider is required to obtain the Information Security Management System ("**ISMS**") certification, i.e., the IT Service Provider meets one of the following thresholds:

    (i) Its annual revenue from telecommunications services exceeds KRW 10 billion (approx. USD 9 million); or
    (ii) Its average number of daily users over the past three months is at least one million.

2. Holding Concurrent Offices for CISO and CPO

Under Article 45-3(3) of the current IT Network Act, CISOs of IT Service Providers meeting one of the following thresholds are prohibited from holding any other concurrent positions such as COO, CFO and/or even CPO:

(1) The IT Service Provider's total assets amount to at least KRW 5 trillion (approx. USD 4.5 billion); or
(2) the IT Service Provider's total assets amount to at least KRW 500 billion (approx. USD 450 million), and the IT Service Provider is required to obtain the ISMS certification, i.e., the IT Service Provider meets one of the following thresholds:

    (i) Its annual revenue from telecommunications services exceeds KRW 10 billion (approx. USD 9 million); or
    (ii) Its average number of daily users over the past three months is at least one million.

In particular, the current prohibition against CISO's holding a concurrent office for CPO has been the subject of much controversy.

Under the amendments, CISOs will be allowed to hold concurrent positions as CPO, a separate office required under the Personal Information Protection Act which is the overarching data protection and privacy law. As amended, some of the duties that may be performed by a CISO holding concurrent positions have been expanded to include: (i) the duties relating to public disclosure of data protection pursuant to the Act on the Promotion of Information Security Industry, (ii) the duties as the chief information security officer under the Act of the Protection of Information and Communication Infrastructure, and (iii) the duties as the chief information security officer under the Electronic Financial Transactions Act.

3. Introduction of Penalty for Non-compliance with the Requirements Relating to Appointment and Concurrent Offices of CISO

Under the current IT Network Act, there is practically no direct penalty for non-compliance with the required qualifications for CISOs and/or CISOs' holding concurrent offices where concurrent office is prohibited. This is because MSICT only has the authority to issue corrective orders and to issue an administrative fine (i.e., up to KRW 30 million (approx. USD 27,000)) only if such order is not complied with. Meanwhile, failure to report the appointment of the CISO may lead to an administrative fine of up to KRW 30 million (approx. USD 27,000).

Under the amended IT Network Act, however, designating a CISO who does not meet the statutory qualifications, having CISO hold concurrent positions where concurrent office is prohibited, and/or the failure to report the appointment of CISO will each be subject to an administrative fine of up to KRW 30 million (approx. USD 27,000) even in the absence of a corrective order issued by MSICT.

4. Going Forward

The amended IT Network Act will come into effect 6 month after its promulgation or towards the end of this year. Although the practical impact of the amendments will become more apparent once the specific criteria under the relevant Presidential Decree have been legislated, the amendments are expected to relax the burden on IT Service Providers by removing the need to designate full-time, executive-level CISOs whose sole function is to serve as the CISO.

BKL has extensive experience in handling compliance and enforcement of the IT Network Act and the Personal Information Protection Act, including appointment of CISO and reporting thereof to MSICT. For any inquiry or question regarding the content of this newsletter, please contact us.