SHIN&KIM
법무법인(유) 세종

중국 데이터 보안법 제정과 시사점

2021.07.27

Ⅰ. 서론

중국 데이터 보안법(数据安全法, 이하 “데이터 보안법”)이 2021년 6월 10일 중국 제13기 전국인민대표대회 상무위원회 제29차 회의를 통과하여 제정되어 9월 1일 시행을 앞두고 있습니다. 본 뉴스레터에서는 데이터 보안법의 주요 내용을 소개해드리고 시사점에 대해 말씀드리고자 합니다.

Ⅱ. 데이터 보안법의 주요 내용

1. 적용범위와 관련 개념

(1) 적용범위

데이터 보안법은 중화인민공화국 경내(境内, 경내라 함은 홍콩, 마카오, 대만을 제외한 중국 대륙을 의미하며, 이하 동일합니다)에서의 데이터 처리 활동 및 그 보안에 대한 관리감독에 대해서 규정하고 있습니다(데이터 보안법 제2조). 나아가 중화인민공화국 경외에서의 데이터 처리 활동이 중화인민공화국의 국가안전, 공공이익 또는 공민, 조직의 합법적인 권익을 침해하는 경우에는 데이터 보안법에 따라 법적 책임을 부담하도록 규정하여 데이터 보안법의 경외적용 가능성에 대해서도 규정하고 있습니다(데이터 보안법 제2조). 한편 국가비밀과 관련된 데이터 처리 활동에는 중화인민공화국 국가비밀 보호법 등의 법률 및 관련 행정법규(입법기관이 만든 법률이 아니라 행정기관이 만든 규정을 의미합니다)를 적용하고(데이터 보안법 제53조), 통계나 문서보존 업무상 데이터 처리를 하거나, 개인정보와 관련된 데이터 처리를 하는 경우에는 관련 법률 및 행정법규를 준수하도록 요구하고 있습니다(데이터 보안법 제53조).

(2) 데이터 및 보안의 개념

데이터 보안법에서 말하는 “데이터”란 전자 또는 기타 방식으로 이루어진 정보에 관한 모든 기록을 말합니다. “데이터 처리”에는 데이터의 수집, 저장, 사용, 가공, 전송, 제공, 공개 등이 포함되며, “데이터 보안”이란 필요한 조치를 통해서 데이터를 효과적인 보호 및 합법적인 이용 상태에 두거나 지속적인 보안 상태를 담보할 수 있는 능력을 구비하는 것을 말합니다(데이터 보안법 제3조). 데이터 보안법에서는 “국가 핵심 데이터(国家核心数据)”라는 용어가 처음 등장했는데 국가안전 및 국민경제의 근간, 중요한 민생, 중대한 공공이익 등과 관련된 데이터는 국가 핵심 데이터에 속하며 상당히 엄격한 관리제도를 통한 특별한 보호를 받게 됩니다. 또한 중국 각 지방정부 및 부서는 데이터 분류 등급 보호제도에 따라 해당 지방정부 및 부서와 관련된 산업 및 분야의 중요 데이터(重要数据)의 구체적인 목록을 정하고 이러한 데이터에

대해서는 중점적으로 보호하도록 규정하고 있습니다(데이터 보안법 제21조).

(3) 데이터 처리 활동에 관한 권리와 의무

데이터 처리 활동은 법률 및 행정법규를 준수하고 사회의 공중도덕과 윤리를 존중하고 상도덕과 직업 윤리를 준수하며 신의성실, 데이터 보안 관련 의무를 이행해야 합니다. 또한 사회적 책임을 이행하고 국가안전, 공공이익에 해를 끼쳐서는 안 되며 개인조직의 합법적인 권익에 손해를 끼쳐서도 안 됩니다(데이터 보안법 제8조).

개인이나 조직은 데이터 보안법의 규정에 위반한 행위를 관련 주무부서에 신고 내지 고발할 수 있고, 신고 내지 고발을 접수한 부서는 이를 적시에 관련 법에 따라 처리해야 하며, 신고 내지 고발인의 신상정보에 대해서는 비밀을 유지해야 하고, 신고 내지 고발인의 합법적인 권익을 보호해야 합니다(데이터 보안법 제12조).

개인이나 조직은 데이터를 수집할 때에는 합법적이고 정당한 방식을 통해야 하고 절취 또는 기타 불법적인 방법으로 데이터를 취득해서는 안 됩니다. 법률, 행정법규에 데이터의 수집 사용의 목적, 범위에 관한 규정이 있는 경우에는 그 목적과 범위 내에서 데이터를 수집, 사용해야 해야 합니다(데이터 보안법 제32조).

한편 공안, 국가보안기관이 법에 따라 국가 안보의 수호 또는 범죄 수사의 필요에 따라 데이터를 수집하는 경우에는 관련 규정에 따른 승인 절차 등의 법적 절차를 준수해야 하며 관련 조직이나 개인은 이에 협조해야 합니다(데이터 보안법 제35조).

(4) 데이터의 국경간 이동

중화인민공화국 주무부서는 관련 법률과 중화인민공화국이 체결 또는 참가한 국제조약, 협정 또는 평등 호혜의 원칙에 따라 외국 사법 또는 법 집행기구의 데이터 제공에 관한 요청을 처리합니다. 중화인민공화국 주무부서의 승인을 거치지 않으면 경내의 조직이나 개인은 외국의 사법 또는 법 집행기구에게 중화인민공화국 경내에 보존된 데이터를 제공해서는 안 됩니다(데이터 보안법 제36조).

2. 데이터 보안제도

(1) 데이터 등급분류 및 국가안전심사

국가는 데이터에 관한 분류와 등급보호제도를 구축합니다. 즉, 데이터의 경제사회발전 과정에서의 중요도와 일단 변조, 훼손, 누설, 불법획득 또는 이용되면 국가안전, 공공의 이익 또는 개인 내지 조직의 합법적인 권익에 초래될 수 있는 위해의 정도에 따라 데이터에 대한 분류 및 등급 보호를 실시합니다. 또한 국가는 데이터 보안심사제도를 수립하여 국가안전에 영향을 주거나 영향을 줄 가능성이 있는 데이터의 처리 활동에 대해서는 국가안전 심사를 진행합니다. 이 때 이 법에 따라 내려진 안전심사 결정은 최종결정이 됩니다(데이터 보안법 제24조).

(2) 데이터 관련 물품 수출 통제

국가안전과 이익의 수호, 국제적인 의무 이행과 관련이 있는 통제물품에 관한 데이터에 대해서는 법에 따라 수출 통제를 시행합니다(데이터 보안법 제25조). 어떤 국가 또는 지역이 데이터와 데이터 이용기술 등과 관련이 있는 투자, 무역 등의 영역에서 중화인민공화국에 대한 차별적인 금지, 제한 또는 기타 유사한 조치를 취하는 경우에는 중화인민공화국은 실제 상황에 따라 해당 국가 또는 지역 등에 그와 상응하는 조치를 취할 수 있습니다(데이터 보안법 제26조).

(3) 데이터 보안관리 제도

데이터 처리 활동은 법률, 행정법규에 따라 그 모든 과정에서 데이터 보안관리 제도를 수립 내지 완비하고 데이터 보안과 관련한 교육을 실시하며 데이터의 보안관리에 필요한 기술적 조치와 기타 필요한 조치를 취해야 합니다. 인터넷 등의 정보 네트워크를 이용한 데이터 처리 활동에는 네트워크 보안 등급 보호제도를 바탕으로 위와 같은 데이터 보안 의무를 이행해야 합니다. 특히 중요 데이터의 처리자는 데이터 보안 책임자와 관리조직을 명확히 지정하여 데이터 보안 책임을 이행해야 합니다(데이터 보안법 제27조).

3. 데이터 활동에 대한 모니터링 강화 및 중요 데이터의 국내 보존

데이터 처리 시에 리스크에 대한 모니터링을 강화해야 하고, 데이터 보안에 결함 내지 공백 등의 리스크를 발견한 경우에는 즉시 구제조치를 취해야 하며, 데이터 보안 사건이 발생한 경우에는 즉각 필요한 조치를 취하고, 규정에 따라 적시에 사용자에게 고지하는 한편 관련 주무부서에 보고해야 합니다(데이터 보안법 제29조). 중요 데이터의 처리자는 규정에 따라 데이터 처리 활동에 대한 정기 리스크 평가를 진행해야 하고 관련 주무부서에 리스크 평가 보고를 해야 합니다. 리스크 평가 보고는 처리한 중요 데이터의 종류, 수량, 데이터 처리활동의 진행 상황, 당면한 데이터 보안 리스크와 그 대응조치 등의 내용을 포함해야 합니다(데이터 보안법 제30조).

핵심정보기초설비(Critical Information Infrastructure, 일단 파괴되거나 그 능력을 상실하여 데이터가 누설되면 국가안보, 국가의 계획과 민생, 공공이익에 심각한 위해를 가져올 수 있는 네트워크 시설과 정보 시스템으로 공공통신과 정보 서비스, 에너지, 교통, 수리, 금융, 공공서비스, 전자행정, 위생의료, 교육, 사회보험, 환경보호, 클라우딩 컴퓨터, 빅데이터, 국방과학공업, 대형장비, 화공, 식품약품, 신문 등의 영역이 포함됨)의 운영자는 중화인민공화국 경내에서 해당 설비의 운영 중에 수집 생산된 중요데이터의 출경(出境) 보안관리에 대해 중화인민공화국 네트워크 보안법(网络安全法)의 규정을 준수해야 합니다. 네트워크 보안법에 따르면 핵심정보기초시설의 운영자는 중화인민공화국 경내에서 운영 중에 수집 또는 생산한 개인정보와 중요데이터를 경내에 보존해야 하고, 업무상 경외 제공이 명백히 필요한 경우에는 국가 인터넷 정보 부서와 국무원 관련 부서가 제정한 방법에 따라 보안평가를 실시하는 한편 법률, 행정법규에 별도의 규정이 있는 경우에는 그 규정에 따라야 합니다(네트워크 보안법 제37조). 기타 데이터 처리자가 중화인민공화국 경내에서 수집 내지 생산한 중요데이터에 관한 출경(出境) 보안관리 방법은 국가 인터넷 정보 부문이 국무원의 관련 부서와 함께 제정합니다(데이터 보안법 제31조).

III. 해외 상장 중국기업에 대한 네트워크 보안심사제도의 도입

1. 해외 상장 중국기업에 대한 네트워크 보안심사 통보

최근 중국의 대표적인 자동차 공유 APP인 띠디추싱(滴滴出行)이 미국 나스닥 시장에 상장된 것과 관련하여 중국 정부는 중국 내 APP스토어에 띠디추싱 APP를 퇴출시키라는 지시를 내리고 띠디추싱에는 네트워크 보안심사를 통보했습니다. 띠디추싱이 미국에 상장을 진행하는 과정에서 중국의 지도와 중국인들의 이동에 관한 다량의 정보가 국외로 유출되었다는 것이 중국 당국의 판단인 듯 합니다.

현행 네트워크 보안심사방법(网络安全审查办法) 제15조는 감독관리 기구가 국가 안보에 영향을 미칠 수 있다고 판단한 네트워크 제품과 서비스에 대해서는 직권에 따라 보안심사를 진행할 수 있도록 규정하고 있고, 국가안전법(国家安全法) 제59조는 국가안보에 영향을 주거나 또는 영향을 줄 가능성이 있는 네트워크 정보기술 제품과 서비스에 대해 국가보안심사를 할 것을 요구하고 있습니다. 중국 당국은 이러한 규정에 근거하여 띠디추싱에 네트워크에 관한 보안심사를 통보한 것으로 보입니다.

2. 네트워크 보안심사방법(개정안의 의견수렴안) 공포

이에 한걸음 더 나아가 2021년 7월 10일 중국의 국가 인터넷 사무처는 네트워크 보안심사방법(개정안의 의견수렴안) 《网络安全审查办法（修订草案征求意见稿）》(이하 "본 개정안"이라 약칭합니다)을 반포했습니다. 본 개정안은 제6조를 신설하여 100만명 이상의 개인정보를 보유하고 있는 운영자가 국외에 상장을 하려는 경우에는 반드시 네트워크 보안심사 사무처에 네트워크 보안심사를 요청하도록 했습니다. 이를 위해 네트워크 보안심사 기구에 증권감독관리위원회를 추가하여 국외에 상장하려는 중국기업들을 감독하도록 했습니다.

현행 네트워크 보안심사방법이 주로 핵심정보기초설비 운영자에게 적용되는 것에 반해, 본 개정안은 보안심사 대상을 데이터 처리 업무에 종사하는 데이터 처리자로 대폭 확대하였습니다. 본 개정안에서는 데이터 보안법을 근거 법률로 새롭게 추가하였는데, 데이터 보안법에 따르면 표현 방식이 전자적 방식이든 기타 방식이든, 데이터의 수집이 인터넷을 통해 이루어지든 그렇지 않든 모두 데이터에 해당하고, 데이터의 내용도 국가 핵심 데이터, 중요 데이터, 기타 데이터 등으로 광범위하게 규정되어 있기 때문에, 네트워크 보안심사의 대상 범위가 상당히 확대되는 결과가 될 것입니다. 본 개정안은 데이터 보안법과 함께 중국이 자국 내 데이터의 국외 반출에 대한 관리감독을 함에 있어 중요한 근거규정이 될 것으로 보입니다

VI. 시사점

데이터 보안법은 국가가 데이터 거래관리제도, 데이터 보호제도, 데이터 보안 리스크 통제제도, 데이터 보안 응급조치 시스템 구축, 데이터 보안심사제도 등 데이터 처리 활동과 관련한 각종 제도를 시행하도록 규정하고 있습니다. 그 결과 데이터 보안법은 물론 신규로 시행되는 제도들은 중국과 관련된 데이터를 수집하고 이용하는 등 사업자의 영업 과정에서 데이터를 처리하는 행위에까지 직·간접적으로 영향을 미칠 수 있습니다. 나아가, 데이터 보안법은 지역별, 업종별로 데이터의 처리에 관한 관리감독의무를 부과하고 있는 바, 중국과 관련된 데이터를 처리하고 있거나 처리하려는 사업자로서는 곧 시행을 앞두고 있는 데이터 보안법 및 신규 제도에 따른 규제 리스크를 사전에 면밀히 검토할 필요가 있어 보입니다.

관련구성원

허욱
변호사

02-316-1723
whuh@shinkim.com

원중재
변호사

+86-10-8447-5343
jjwon@shinkim.com