



중국의 데이터 경외이전 보안평가방법의 시행과 시사점

2022.09.07

2022년 5월 19일 중국의 국가 인터넷 정보 사무처 실무회의에서 데이터 경외 이전 보안평가 방법 《数据出境安全评估办法》(이하 “본 보안평가방법”이라고 약칭함)이 통과되어 2022년 9월 1일부터 시행되었습니다. 국경을 초월해 넘나드는 데이터는 이제 미래의 먹거리로 그 경제적인 가치를 인정받고 있고 메타버스로 대표되는 가상세계에서의 데이터의 생성과 활용으로 인해 각 국가들은 보이지 않는 영역에서도 주도권 쟁탈을 가속화하고 있습니다. 중국과 인접하여 많은 인적 물적 교류를 이어온 우리나라로서는 데이터의 왕래가 필연적인 상황이기 때문에 본 보안평가방법의 반포와 시행에 각별한 주의를 기울일 필요가 있습니다. 본 뉴스레터에서는 본 보안평가방법의 주요내용을 설명드리고 시사점을 말씀드리고자 합니다.

I. 본 보안평가방법의 주요 내용

1. 본 보안평가방법의 적용 범위—데이터의 경외 이전

본 보안평가방법은 데이터 처리자가 경외¹로 중화인민공화국 경내에서 수집 내지 생산한 중요 데이터와 개인정보를 역외로 제공할 때의 보안평가에 적용됩니다. 단, 법률, 행정법규에 별도의 규정²이 있는 경우에는 그 규정에 의합니다(제2조). 본 보안평가방법에서 말하는 중요데이터란 일단 변조, 파괴, 누설 또는 불법적으로 획득되거나 이용되는 경우에는 국가보안, 경제운용, 사회 안정, 공공의 건강과 안전 등에 위해를 끼칠 수 있는 데이터를 말합니다(제19조).

한편 7월 7일 본 보안평가방법의 반포에 즈음하여 개최된 기자회견에서 인터넷 정보 사무처 담당자는 본 보안평가방법에서 규정한 데이터의 경외 이전의 두 가지 상황을 언급했는데 첫째는 데이터 처리자가 경내에서 수집 내지 생산한 데이터를 경외로 전송하거나 경외에 보관하는 경우이고, 둘째는 데이터 처리자가 수집 내지 생산한 데이터를 경내에 보관하고 경외의 기구, 조직 또는 개인이 접근 또는 사용할 수 있는 경우입니다.

2. 데이터 경외이전의 보안평가 방법—자체 보안평가 및 관할부서의 보안평가

가. 자체 보안평가

데이터 처리자는 데이터 경외 이전을 위한 당국의 보안평가를 진행하기 전에 데이터의 경외 이전에 관한 자체 보안평가를 실시해야 합니다

. 자체 보안평가에는 (1) 데이터 경외이전과 경외 수령자의 데이터 처리 목적, 범위, 방식 등의 합법성, 정당성, 필요성, (2) 경외 이전 데이터의 규모, 범위, 종류, 민감 정도, 데이터 경외이전이 국가안전, 공공이익, 개인 또는 조직의 합법적인 권익에 야기할 수 있는 리스크, (3) 경외 수령자가 부담하기로 약속한 책임 내지 의무와 그 책임과 의무를 이행하기 위한 관리와 기술적인 조치와 능력 등이 경외로 이전한 데이터의 보안을 보장할 수 있는지 여부, (4) 데이터가 경외로 이전된 후에 변조, 파괴, 누설, 분실, 재이전 또는 불법적으로 취득 내지 이용될 리스크, 개인정보의 권리와 이익을 보호하는 채널이 원활한 지 여부 등, (5) 경외 수령자와 체결하고자 하는 데이터 경외 이전 관련 계약 또는 기타 법률적 효력을 가지고 있는 문건 등(이하 “법률문건”으로 통칭함)에 데이터 보안에 관한 책임과 의무가 충분히 규정되어 있는지 여부, (6) 데이터의 경외 이전과 관련한 보안에 영향을 줄 수 있는 기타 사항이 중점 평가사항에 해당합니다(제5조).

나. 관할부서의 보안평가

데이터 처리자의 경외 데이터 제공이 (1) 경외에 중요데이터를 제공하는 경우, (2) 핵심정보기초시설 운영자³와 100만명 이상의 개인정보 데이터 처리자가 경외로 개인정보를 제공하는 경우, (3) 전년도 1월 1일부터 경외로 누적 10만명 이상의 개인정보를 제공하거나 1만명 이상의 민감개인정보의 데이터 처리자가 경외로 개인정보를 제공하는 경우, (4) 국가 인터넷 정보부서에서 규정한 기타 데이터 경외이전 보안평가 신고 대상에 해당하는 경우에는 소재지의 성급 인터넷 정보 부서를 통해 국가 인터넷 정보부서에 데이터 경외이전 보안평가를 신청해야 합니다(제4조). 한편 데이터 경외이전 보안평가 신고에는 (1) 신청서, (2) 데이터 경외이전 리스크와 관련한 자체평가보고, (3) 데이터 처리자와 경외 수령자간에 체결된 법률문건, (4) 보안평가 업무에 필요한 기타 자료를 제출해야 합니다.

다. 보안평가의 대상

데이터 경외이전 보안평가는 데이터의 경외이전이 국가안전, 공공의 이익, 개인 또는 조직의 합법적인 권리와 이익에 야기할 수 있는 리스크를 중점적으로 평가하는데, (1) 데이터 경외 이전의 목적, 범위, 방식 등의 합법성, 정당성, 필요성, (2) 경외 수령자의 소재국가 또는 지역의 데이터 보안 보호정책법규와 네트워크 보안 환경이 경외로 이전된 데이터 보안에 미치는 영향, 경외 수령자의 데이터 보호 수준이 중화인민공화국 법률, 행정법규의 규정과 강제적 국가 표준의 요건에 부합하는지 여부, (3) 경외이전 데이터의 규모, 범위, 종류, 민감 정도, 경외 이전 과정과 송출 후에 변조, 파괴, 누설, 분실, 이전 또는 불법적으로 취득 내지 이용될 리스크, (4) 데이터 보안과 개인정보의 권리와 이익이 충분하고 효과적으로 보장을 받을 수 있는지 여부, (5) 데이터 처리자와 경외 수령자 간에 체결한 법률문건이 데이터 보안 및 보호의무를 충분히 규정하고 있는지 여부, (6) 중국의 법률, 행정법규, 부문규장의 준수 상황, (7) 국가 인터넷 정보 부서가 평가가 필요하다고 판단한 기타 사항이 주요 평가 대상에 포함됩니다(제8조).

3. 데이터 경외이전의 보안평가 절차

가. 보안평가 절차

성급 인터넷 정보 통신부서는 신청자료를 수령한 날로부터 5영업일 이내에 신청서류가 완비되었는지 여부에 관한 검사를 마치고 신청서류가 모두 구비된 경우에는 신청서류를 국가 인터넷 정보 부서에 송부합니다. 신청서류가 미비한 경우에는 데이터 처리자에게 반환하고 보완이 필요한 자료를 고지합니다. 국가 인터넷 정보 부서는 신청자료를 수령한 날로부터 7영업일 내에 데이터 처리자의 신청을 수리하고 수리통지 여부를 결정해야 합니다(제7조).

보안평가 과정에서 데이터 처리자가 제출한 신고자료가 요건에 부합하지 않는 경우에는 국가 인터넷 정보 부서는 보완 또는 수정을 요구할 수 있습니다. 데이터 처리자가 정당한 이유 없이 보완이나 수정을 하지 않는 경우에는 국가 인터넷 정보 부서는 보안평가를 종료할 수 있습니다. 데이터 처리자는 그가 제출한 자료의 진실성에 대한 책임을 지고 고의로 허위 자료를 제출한 경우에는 보안평가를 통과할 수 없고 법에 따라 상응한 책임을 부담해야 합니다(제11조).

국가 인터넷 정보부서는 데이터 처리자에게 보안평가에 관한 서면 수리통지서를 발급한 날로부터 45영업일 내에 데이터 경외이전에 관한 보안 평가를 완료해야 합니다. 상황이 복잡하거나 또는 자료의 보안이나 수정이 필요한 경우에는 보안평가 기간을 적절하게 연장하고 이를 고지할 수 있습니다. 평가결과는 서면으로 데이터 처리자에게 통지해야 합니다(제12조). 데이터 처리자가 평가 결과에 이의가 있는 경우에는 평가결과를 수령한 날로부터 15영업일 내에 국가 인터넷 정보 부서에 재심을 신청할 수 있습니다. 재심결과는 최종적인 결정으로 이의를 제기할 수 없습니다(제13조).

나. 데이터 처리자와 경외 수령자 간의 법률문건

데이터 처리자와 경외 수령자 간에 체결된 법률문건에는 최소한, (1) 데이터 경외이전의 목적, 방식과 데이터의 범위, 경외 수령자의 데이터 처리의 용도와 방식 등, (2) 데이터의 경외 보존 지점 및 기한과 데이터 보존기한이 만료되었을 때, 약정한 목적을 완성했을 때 또는 법률문건의 효력이 종료한 후에 경외로 이전한 데이터에 대한 조치방안, (3) 경외 수령자가 경외 이전한 데이터를 다시 다른 조직 내지 개인에게 재이전하는 경우 준수해야 하는 요건, (4) 경외 수령자의 실제 통제권 또는 경영범위에 발생한 실질적인 변화 또는 소재지 국가 내지 지역의 데이터 보안 및 보호 정책법규와 네트워크 보안 환경의 변화와 기타 불가항력적인 사유로 인해 데이터 보안을 담보하기 어려운 경우에 취해야 하는 안전조치, (5) 법률 문건에 규정된 데이터 보호의무를 위반하는 경우의 구제조치, 계약위반시 책임과 분쟁의 해결 방식, (6) 경외 이전한 데이터가 변조, 파괴, 누설, 분실, 재이전 또는 불법적으로 획득 또는 이용될 리스크가 있는 경우에 취해야 할 긴급조치 방안 및 개인이 그 개인정보의 권리와 이익을 보호할 수 있는 채널과 방식과 같은 내용이 포함되어야 합니다(제9조).

다. 보안평가의 유효기한 및 재평가

데이터 경외 이전 보안평가 결과의 유효기한은 2년으로 평가결과서가 발급된 날로부터 기산됩니다. 유효기한 동안에도 (1) 경외로 데이터를 제공하는 목적, 방식, 범위, 종류와 경외 수령자의 데이터 처리의 목적과, 방식에 변화가 발생하여 경외로 이전한 데이터의 보안에 영향을 주는 경우, 또는 개인정보와 중요데이터의 경외 보존기한이 연장되는 경우, (2) 경외 수령자의 소재국가 또는 지역의 데이터 보안 및 보호 정책법규와 네트워크 보안 환경에 변화가 발생하고 기타 불가항력적인 상황의 발생으로 데이터 처리자 또는 경외 수령자의 실제 통제권에 변화가 발생한 경우, 데이터 처리자와 경외 수령자 간의 법률문건의 변경 등 경외로 이전한 데이터 보안에 영향을 주는 사유가 발생한 경우, (3) 경외로 이전한 데이터의 보안에 영향을 주는 기타 상황이 발생한 경우에는 데이터 처리자는 재평가를 신청해야 합니다.

한편, 유효기한이 만료한 후에도 데이터 경외 이전 활동을 계속할 필요가 있는 경우에는 데이터 처리자는 유효기한의 만료 전 60영업일 전에 재평가를 신청해야 합니다(제14조). 국가 인터넷 정보 부서는 이미 보안평가를 거쳐 경외로 이전한 데이터가 실제로 처리되는 과정에서 데이터 경외 이전 보안 관리 요건에 부합하지 않게 된 경우에는 서면으로 데이터 처리자에게 데이터 경외이전 활동을 중지할 것을 통지할 수 있습니다(제17조).

II. 시사점

1. 중국은 2017년 6월 1일부터 네트워크 보안법, 2021년 9월 1일부터 데이터 보안법, 2021년 11월 1일부터 개인정보보호법을 시행하면서 이른바 데이터 3법 체계를 완성했습니다. 네트워크안전법 제37조는 원칙적으로 핵심정보기초시설의 운영자는 중화인민공화국 경내에서 수집 또는 생산한 개인정보와 중요데이터를 경내에 보존하도록 규정하고 있습니다. 그리고 업무상 필요로 경외 제공이 필요한 경우에는 국가 인터넷 정보 부서와 국무원 관련 부서가 제정한 방법에 따라 보안평가를 실시하도록 규정하고 있는데 본 방법은 위 규정에 근거하여 제정된 세부적인 규정에 해당합니다.
2. 본 방법은 2022년 9월 1일부터 시행되었는데 본 방법 제20조는 본 방법 시행 전에 이미 실시한 데이터 국외 이전이 본 방법에 부합하지 않는 경우에는 본 방법의 시행일로부터 6개월 내에 개선을 완료하도록 소급효에 대해서도 규정하고 있습니다. 그런데 본 방법은 소급효가 언제까지 미치는지에 관한 명확한 규정이 없습니다. 즉, 본 방법이 시행된 2022년 9월 1일 이전의 어떤 시점의 행위에

대해서까지 본 방법의 시행 후 6개월이 되는 시점인 2023년 3월 1일 이전에 본 방법에 따른 보안평가를 완료하여야 한다는 것이인지가 불명확합니다. 이 부분은 향후 본 방법이 시행된 이후 집행당국의 입장을 잘 모니터링 할 필요가 있습니다.

3. 본 보안평가방법의 대상이 되는 데이터의 경외 이전에는 데이터 처리자가 수집 내지 생산한 데이터를 경내에 보관하고 경외의 기구, 조직 또는 개인이 이를 접근 또는 사용할 수 있는 경우도 포함됩니다. 즉, 데이터를 물리적으로 경외로 이전하는 것뿐만 아니라 경외의 조직이 경내 서버에 접속하여 조사연구를 하는 경우도 이를 데이터 경외 이전으로 보고 있습니다. 그렇기 때문에 한국의 본사가 중국의 자회사의 데이터 서버에 접근하려는 경우에도 중국 자회사는 본 보안평가방법의 요건에 해당하면 보안평가를 받은 후에 한국 본사의 접속을 허용해야 할 것으로 보입니다.
4. 본 보안평가방법에 의하면 데이터 보안 평가의 유효기한은 2년이고 2년이 만료되기 60일 전에 재평가를 신청해야 합니다. 그런데 2년의 유효기간 동안에도 경외로 이전한 데이터의 보안에 영향을 주는 중대한 상황변화가 발생한 경우에는 그로부터 60일이 경과할 때까지 재평가를 받아야 하며 그 기간 내에 재평가가 완료되지 않으면 데이터의 경외이전을 중단해야 하는 상황이 생길 수 있고, 이로 인해 사업 수행에 중대한 차질이 발생할 수도 있습니다. 그렇기 때문에 데이터를 경외로 이전해야 하는 기업은 자신들이 경외로 이전해야 하는 데이터의 상황 변화, 경외 수령자의 변화, 경외 수령자 소재지 국가 또는 지역의 데이터 보안 및 보호 법률정책의 변화를 평소에 잘 파악하고 사전에 보안평가의 유효기간 만료에 대비한 재평가를 준비해야 합니다.
5. 중국의 데이터 처리자가 한국의 데이터 수령자와 법률문건을 통해 데이터를 경외로 이전하는 경우 법률문건에는 경외 수령자의 소재지 국가 즉, 한국의 데이터 보안 및 보호 정책법규와 네트워크 보안 환경에 대한 변화와 기타 불가항력적인 사유로 인해 데이터 보안을 담보하기 어려운 경우에 취해야 하는 안전 조치 등도 기재할 것을 요구하고 있습니다. 따라서 중국의 데이터를 한국으로 이전하는 경우에는 본 보안평가방법을 포함한 중국의 관련 법규뿐만 아니라 한국의 데이터 보호법제의 변화도 잘 파악하고 있어야 함을 주의해야 합니다.
6. 본 보안평가방법의 시행으로 중국 내에서 수집 및 생성된 데이터의 경외 이전 및 경외에 소재한 기구, 조직, 개인의 중국 내 데이터 접근 및 사용에 대한 보안평가 방식이 구체화됨에 따라 그 동안 다양한 방식으로 중국 내 데이터를 활용해 오던 한국기업 입장에서는 현재까지의 데이터 활용 방식이 본 보안평가방법의 요건에 부합하는지 등에 대한 면밀한 검토가 필요한 상황입니다. 아울러 본 보안평가방법에 규정된 보안평가의 요건과 방식이 상당히 까다롭고 추상적이어서 중국 관련 부서의 재량의 여지가 큰 만큼(즉, 보안 평가에 통과할 수 있을지 여부에 대한 보장이 어려울 수 있음), 향후 중국 내 사업수행 과정에서 수집 및 생성된 데이터를 어떻게 관리할 것인지에 대해서도 보다 전략적인 고민이 필요할 것으로 보입니다.
7. 특히 보안평가 진행을 위해서는 중국 내 관련 법규정의 내용 및 변화는 물론 정보이용자가 소재한 한국의 데이터 보안 및 보호 정책법규와 네트워크 보안 환경에 대한 내용 및 변화에 대해서도 숙지하고 있어야 한다는 점에서, 향후 중국 내 데이터 관리에 대한 한국 기업들의 컴플라이언스 측면에서의 강도높은 관심과 주의가 필요하다고 하겠습니다.

¹ 경외(境外)라 함은 중국 본토 대륙 이외의 지역으로 홍콩, 대만, 마카오를 포함합니다.

² 예를 들면 기업이 이전하려는 데이터가 국가기밀과 관련이 있는 경우에는 중화인민공화국 국가기밀 보호법 《中华人民共和国保守国家秘密法》 제 30조에 따라 국무원의 관련 부서, 성, 자치구, 직할시 인민정부의 관련 부서의 비준을 얻고 상대방과 비밀유지계약을 체결한 이후에 비로서 제공이 가능합니다.

³ 중국의 네트워크안전법 제31조와 ‘핵심정보기초시설안전보호조례’ 《关键信息基础设施安全保护条例》에 따르면 핵심정보기초시설(关键信息基础设施, Critical Information Infrastructure, 영문으로 통상 “CII”라고 약칭함)이란 일단 파괴되거나 그 능력을 상실하거나 또는 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, 클라우드 컴퓨팅, 빅데이터, 국방과학공업, 대형장비, 화공, 식품약품, 신문 등의 영역이 포함됩니다.

관련구성원

원중재

변호사

+86-10-8447-5343

jjwon@shinkim.com

정천주

외국변호사

02-316-4201

tszheng@shinkim.com

허욱

변호사

02-316-1723

whuh@shinkim.com

장대훈

외국변호사

+86-10-8447-5343

dxzhang@shinkim.com