中倫
ZHONG LUN

《사이버 보안법》시행 전 기업 준비사항

중룬 변호사사무소 - 2017

강사 소개

전화:
+86-10 5957 2288

이메일:
chenjihong@zhonglun.com

중룬 사무실:
베이징 - 상하이 - 선전 - 광저우
우한 - 홍콩 - 도쿄 - 런던

천지홍 - 중룬 변호사사무소의 파트너

- 전국변호사협회 정보 네트워크 및 하이테크위원회, 부주임
- 베이징 변호사협회 전기통신법률위원회, 주임
- 국가 지식재산권 사무소 국가 지식재산권 싱크탱크, 전문가
- 국가 지식재산권 전략사무소, 지식재산권 전략가
- 베이징 주요산업 지식재산권 연맹, 지식재산권 전문가
- 중국 인터넷협회 법치실무위원회, 컨설턴트

천지홍 변호사는 2005년 법제일보 및 중국 전자상거래협회에서 '2005IT 법률가 탑10'에 선정되었다. 2006년 국가 지식재산권 전략사무소에서 국가 지식재산권 전략전문가로 선정되었다. 2011년 영국의 '기업 INTL 매거진'이 선정한 '중국 변호사 탑 50'에 뽑혔다. 2011년, 국가 지식재산권 사무소의 심사를 거쳐 국가 지식재산권 싱크탱크에 들어갔다. 2013년 천지홍 변호사는 베이징 변호사협회에서 '베이징 10대 지식재산권 변호사'의 칭호를 수여 받았다. 2015년 '아시아 법률 및 비즈니스' 단체에서 중국의 15대 지식재산권 변호사로 선정되었고, 2016년, '기업 INT'에서 중국 최고의 전기통신 변호사로 선정되었다.

목차

中倫
ZHONG LUN

《사이버 보안법》 시행 상황

中倫律师事务所
ZHONG LUN LAW FIRM

사이버 보안법의 시행 상황

2016년 11월 7일

전국인민대표대회 상무위원회는《사이버 보안법》을 통과시켰고, 2017년 6월 1일부터 정식 시행하기로 결정했다.《사이버 보안법》은 중국의 사이버 공간 안전을 관리하는 기본 법률이다.

시행 전에 유예 기간이 있는가?

사이버 보안법의 시행 상황

2016년 7월

정부 네트워크 안전 및 정보화 영도소조의 승인을 거쳐서 전국적 범위의 핵심 정보 인프라 네트워크 보안 조사 작업이 시작되었고, 국가 핵심 정보 인프라 네트워크 보안을 위한 전반적이고 기초적인 작업을 실시하였다.

2017년

전국인민대표대회

사이버 보안법 집행에 대한 조사를 실시하였고, 개인 정보 보호 강화에 중점을 두었다.

공안부

네트워크 안전 정보 통보 및 공안기관 사이버 보안법 집행 조사

사이버 보안법의 시행 상황 - 관련 법규

국가인터넷정보사무실

- 《네트워크 제품 및 서비스 보안 심사 방법(초안)》공개적 의견 수렴
- 《데이터 국외 전송 보안 평가 방법》

국무원

《핵심 정보 기초 안보 조항》

부처 입법

《민간항공 네트워크 정보 안전관리 규정(잠행)(초안)》공개적 의견 수렴(2017년 3월)

표준 제정

- GB/T - 정보보안기술 - 네트워크 보안 등급 보호 실시 가이드
- GB/T - 정보보안기술 - 개인 정보 보안 규범

사이버 보안법의 시행 상황 - 집법 부문

中倫
ZHONG LUN

02

《사이버 보안법》 네트워크 운영자

中倫律师事务所
ZHONG LUN LAW FIRM

中倫 ZHONG LUN

네트워크 운영자란?

초안:

네트워크 운영자란 네트워크의 소유자, 관리자 및 타인이 소유 또는 관리하는 네트워크를 이용해 관련 서비스를 제공하는 네트워크 제공자를 가리키며, 기초 전기통신 운영자, 네트워크 정보 서비스 제공업체, 주요 정보시스템 운영자 등을 포함한다.

정식 문서:

네트워크 운영자란 네트워크의 소유자, 관리자 및 네트워크 서비스 공급자이다.

사이트, 플랫폼, 산업 제어, 내부 사무실 네트워크, 해외 네트워크 시스템(국내와 데이터 교환 있음)

네트워크 운영자의 법적 의무 및 책임

- 네트워크 안전 등급 보호 제도(제21조)
- 사용자 정보 보호 제도(제22조 및 제40조)
- 인터넷 실명제(제24조)
- 네트워크 안전사고 응급 대처방안(제25조)
- 개인 정보의 수집과 이용 규칙 제도(제41조 및 제42조)
- 개인 정보 유출사고의 신고 제도(제42조)
- 개인 정보의 불법적인 삭제 및 오류 개인 정보 수정 제도(제43조)
- 네트워크 운영자의 사용자 불법 정보 전파에 대한 관리감독(제47조)
- 네트워크 정보 안전 고발, 신고 제도(제49조)

네트워크 보안 등급 보호 제도

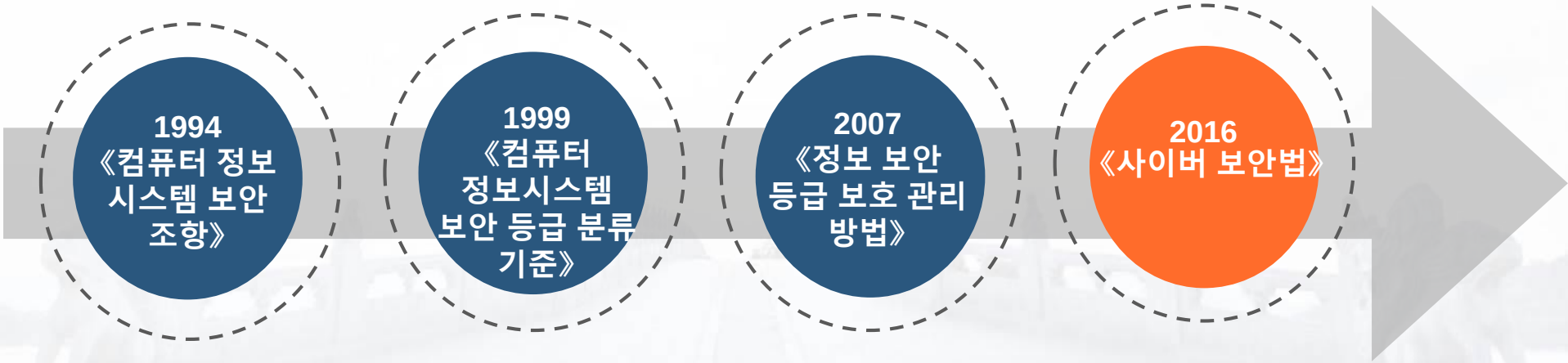
《사이버 보안법》 제21조에 근거해 국가는 네트워크 안전 등급 보호 제도를 실시한다. 네트워크 운영자가 책임지는 네트워크 안전 등급 보호 제도와 관련된 보안 의무는 다음과 같다.

- 내부 안전 관리 제도와 운영 규정을 제정하고, 네트워크 보안 책임자를 세워서 네트워크 보안 책임을 이행한다.
- 컴퓨터 바이러스 및 네트워크 공격, 네트워크 침입 등 사이버 안전을 해치는 행위를 예방하기 위해 기술적 조치를 취한다.
- 네트워크 실행 상태, 네트워크 보안 사고를 모니터링, 기록하는 기술적 조치를 취하고, 규정에 따라 관련 네트워크 일지를 최소 6개월 이상 보관한다.
- 데이터 분류, 핵심 데이터 백업 및 암호화 등 조치를 취한다.
- 법률, 행정 법규가 규정하는 다른 의무.

네트워크 보안 등급 보호 제도

中倫
ZHONG LUN

- **네트워크 보안 등급 보호 제도**
- **정보시스템 보안 등급 보호 제도**



네트워크 보안 등급 보호 제도

中倫 ZHONG LUN

등급	피해 결과			
	사적 권리 (시민, 법인의 합법적 권익)	공공이익	사회 질서	국가 안보
第一级	피해	N	N	N
2등급	심각한 피해	피해	피해	N
3등급		심각한 피해	심각한 피해	피해
4등급		특히 심각한 피해	특히 심각한 피해	심각한 피해
5등급				특히 심각한 피해

1994
《컴퓨터 정보시스템 보안 조항》

中倫律师事务所 ZHONG LUN LAW FIRM

네트워크 보안 등급 보호 제도

中倫 ZHONG LUN

실제 시행 중 정보시스템 등급 확정(참고용):

1등급 정보시스템 : 소규모 개인 경영, 개체 기업, 초중학교, 향진 소속 정보시스템, 현급 단위의 일반 정보시스템에 적용한다.

2등급 정보시스템 : 현급의 모 단위의 중요 정보시스템에 적용한다. 성 직할시 이상의 국가기관, 기업과 사업 단위 내부의 일반적인 정보시스템에 적용한다. 예를 들면, 업무기밀, 상업기밀, 민감한 정보와 상관없는 업무시스템 및 관리시스템 등이다.

3등급 정보시스템 : 일반적으로 성 직할시 이상의 국가 기관, 기업, 사업 단위 내부의 중요 정보시스템에 적용한다. 예를 들면, 영업 비밀, 비즈니스 기밀, 민감한 정보와 관련된 업무시스템 및 관리시스템이다. 성(省)간 또는 전국적 네트워크로 운영하여 생산, 배치, 관리, 명령, 작업, 통제 등 방면에 사용하는 중요 정보시스템 및 성, 성 직할시의 지류 시스템이다. 중앙 각 부처, 성(구, 시) 포털사이트와 중요 사이트 및 성(省)간 연결된 네트워크 시스템 등이다.

4등급 정보시스템 : 일반적으로 국가의 중요한 분야, 부문에서 국가 경제, 국가 이익, 국가 안보와 관련 있고, 사회 안정에 영향을 미치는 핵심 시스템에 적용한다. 예를 들면, 전력 생산 관리 시스템, 은행 핵심 비즈니스 시스템, 통신 핵심 전송 네트워크, 철도 티켓 시스템, 열차 명령 배치 시스템 등이다.

개인 정보 및 그 범위

中倫 ZHONG LUN

개인 정보란 전자 또는 기타 수단으로 기록되어 단독 또는 기타 정보와 결합하여 자연인 개인 신분을 식별할 수 있는 각종 정보를 가리킨다. 자연인의 이름, 생년월일, 신분증 번호, 개인 생물 식별 정보, 주소, 전화 번호 등에 국한되지 않는다.

"처리를 거쳐 특정 개인을 식별할 수 없고 복원할 수 없는 개인 정보는 제외."(제42조)

개인 정보	비 개인 정보
개인 정보	프라이버시
개인 일반 정보	개인 민감한 정보
개인 정보 보호	데이터 보호

VS

개인 정보 보호의 입법 과정

中倫 ZHONG LUN

2009.2

《형법 개정안(7)》

- 시민 개인 정보를 판매하고 불법으로 제공한 죄
- 시민 개인 정보를 불법으로 획득한 죄

2009.12

《권리침해 책임법》

- 프라이버시 권리의 규정
- 성문법에서 프라이버시 권리 개념을 처음으로 열거함

2012.12

《전국인민대표대회 상임위원회의 네트워크 정보 보호 강화에 관한 결정》

- "시민 개인 신분 정보 및 시민 개인 프라이버시에 관련된 전자 정보의 국가 보호"의 법률 원칙을 확립했다.
- 합법적이고 정당하며 필요한 원칙: 명시 + 동의 원칙, 합법적이고 약속에 따른 원칙

2013.2

《개인 정보 보호 가이드》

- 개인 정보 보호의 용어 및 정의 규정
- **개인 정보 처리의 8원칙 제시**
- 개인 정보 주체의 권리 규정

2013.7

《전기통신 및 인터넷 사용자 개인 정보 보호 조항》

- 개인 정보 범위의 정의: 열거 + 요약
- 합법적이고 정당하며 필요한 원칙을 준수하고, 사용자의 개인 정보의 안전을 책임져야 한다.

2014.6

《정보 네트워크를 이용한 개인적 권리 침해 민사 분쟁 안건 심리 적용 법률 몇 가지 문제에 관한 규정》

네트워크 서비스 제공자가 네트워크를 이용해 자연인의 유전자 정보, 의료 기록, 건강검사 자료, 범죄 기록, 집 주소, 개인 활동 및 기타 개인 프라이버시 및 기타 개인 정보를 공개해 타인에게 피해를 끼치고, 권리침해자가 불법 행위 책임을 요구하면 인민법원은 이를 지지한다.

개인 정보 보호의 입법 과정

中倫 ZHONG LUN

2014.3

《소비자 권익 보호법》

경영자 및 그 직원이 수집한 소비자 개인 정보는 엄격하게 보안을 유지하여야 하고, 타인에게 공개, 판매 또는 불법적으로 제공해서는 안 된다. 경영자는 소비자의 동의 또는 요청 없이 또는 소비자가 명확히 거절을 표시한 경우에 상업적 정보를 전송해서는 안 된다.

2015.11

《형법 개정안(9)》

- 범죄 주체 신분의 일반화
- 획득 방법 제한 없음
- 최고 형량은 7년, 처벌 강화.

2016

《사이버 보안법》

- 개인 정보 정의
- 핵심 정보 인프라
- 데이터 국외 전송에 대한 보안 심사

中倫
ZHONG LUN

기본 법적 원칙

- 합법적이고 정당하며 필요한 원칙을 따른다.
- 수집 및 사용 규칙을 공개하고, 정보의 수집, 사용 목적, 방법 및 범위를 명시하며, 수집가의 동의를 거친다.
- 법률, 법규의 규정을 위반하지 않고 양측이 정보의 수집, 사용을 합의한다.

인터넷 실명제 제도

中倫 ZHONG LUN

제24조 네트워크 운영자는 사용자를 위해 네트워크 접속, 도메인 등록 서비스를 처리하고, 유선 전화 및 이동 전화 등 통신사 가입 수속을 하고, 사용자에게 정보 발표, 실시간 통신 등 서비스를 제공한다. 사용자와 계약을 체결하거나 서비스 제공을 확인할 때 사용자에게 실제 신원 정보 제공을 요청하여야 한다. 사용자가 실제 신분 정보를 제공하지 않으면 네트워크 운영자는 관련 서비스를 제공해서는 안 된다.

인터넷 정보 서비스 공급자는 '등록실명제와 아이디 자원설정'의 원칙에 따라 인터넷 정보 서비스 사용자가 신분 정보 인증을 거친 후에 계정 등록이 가능하다.

전자통신, 인터넷, 금융, 숙박, 장거리 여객 운송, 자동차 렌탈 등 사업자, 서비스 제공업체는 고객의 신원을 확인하여야 한다. 신원을 알 수 없거나 신원을 밝히기를 거부한 경우 서비스를 제공해서는 안 된다.

모바일 인터넷 애플리케이션 제공자는 '등록실명제와 아이디 자원설정'의 원칙에 따라 등록된 사용자에게 휴대전화번호 등 실제 신원 정보 인증을 실시한다.

中倫
ZHONG LUN

03 《사이버 보안법》 핵심 정보 인프라 운영자('CII')

中倫律师事务所
ZHONG LUN LAW FIRM

핵심 정보 인프라

中倫 ZHONG LUN

■ 네트워크 보안 법적 의무

1) 핵심 정보 인프라 구축(제33조)

2) 핵심 정보 인프라 운영자의 보안 의무(제34조)

3) 핵심 정보 인프라 제품 및 서비스 구매에 관한 국가 보안 심사(제35조)

4) 핵심 정보 인프라 제품 및 서비스 구매에 관한 기밀(제36조)

5) 개인 정보 및 중요 데이터의 현지화(제37조)

6) 핵심 정보 인프라에 대한 네트워크 보안 연례 평가(제38조)

핵심 정보 인프라

中倫 ZHONG LUN

초안:

공공 통신, 라디오 및 텔레비전 전송 등 서비스를 제공하는 기초 정보 네트워크로, 에너지, 교통, 수자원 관리, 금융 등 중요한 산업과 전원 공급, 급수, 가스 공급, 의료, 사회 보장 등 공공서비스 영역의 중요 정보시스템, 군사 네트워크, 시급 이상 국가기관 등 정부 네트워크, 사용자 수가 많은 네트워크 서비스 제공자가 소유 혹은 관리하는 네트워크와 시스템이다.

두 번째 초안:

파괴, 기능 상실 또는 데이터 유출이 발생하면 국가 안보, 국가 경제, 공공이익을 심각하게 해칠 수 있는 핵심 정보 인프라.

《사이버 보안법》정식 문서

공공 통신 및 정보 서비스, 에너지, 운송, 수자원 관리, 금융, 공공 서비스, 전자 정부 등 국가의 중요 산업과 영역에서 파괴, 기능 상실 또는 데이터 유출이 발생하면 국가 안보, 국민 경제, 공공이익을 심각하게 해칠 수 있는 핵심 정보 인프라로, 네트워크 보안 등급 보호 제도를 기초로 중점적으로 보호한다.

핵심 정보 인프라

中倫 ZHONG LUN

핵심 정보 인프라란 대중에게 네트워크 정보 서비스를 제공하거나 에너지, 통신, 금융, 운송 및 공공 시설과 같은 중요한 산업을 지원하는 정보시스템 또는 산업 제어 시스템을 의미한다. 이런 시스템에 네트워크 보안 사고가 발생하는 경우 중요한 산업의 정상적인 운영에 영향을 미칠 수 있고, 국가의 정치, 경제, 과학기술, 사회, 문화, 국방, 환경 및 사람들의 생명과 재산에 심각한 손실을 초래할 수 있다.

핵심 정보 인프라는 다음과 같다. 정당 및 정부 기관 웹사이트, 기업과 사업 단위 사이트, 뉴스 웹사이트 등과 같은 사이트 류, 실시간 통신, 온라인 쇼핑, 온라인 결제, 검색 엔진, 전자 메일, 포럼, 지도, 오디오 및 비디오 등 네트워크 서비스와 같은 플랫폼 류, 사무와 업무시스템, 산업 제어 시스템, 대형 데이터 센터, 클라우드 컴퓨팅 플랫폼, 텔레비전 전파 시스템과 같은 생산 비즈니스 류가 있다.

-《국가 네트워크 보안 검사 운영 지침》2016.6

핵심 정보 인프라

中倫 ZHONG LUN

3단계 확인

1 핵심 업무 확인

중요 업무를 지원하는 정보시스템 또는 산업 제어 시스템 확인

2

3 핵심업무의 정보시스템 또는 산업 제어 시스템에 대한 의존도 및 정보시스템에 네트워크 보안사고가 발생한 후에 초래할 수 있는 손실에 근거해 핵심 정보 인프라로 확정

A. 사이트 류(《국가 네트워크 보안 검사 운영 지침》)

A. 다음 조건 중 하나가 충족하면 핵심 정보 인프라로 인정한다.

1. 현급 이상 정부 기관 웹사이트. (2016년 조사 중, 모든 정당 및 정부기관 웹사이트는 등록 양식을 작성해야 한다)

2. 중점 뉴스 사이트. (2016년 조사 중, 모든 뉴스 사이트는 등록 양식을 작성해야 한다)

3. 일 평균 방문량이 100만 명 이상인 사이트.

4. 네트워크 보안 사고가 발생할 경우 다음과 같은 영향이 발생할 수 있다.

(1) 100만 명이 넘는 사람들의 일과 삶에 영향을 준다.

(2) 단일 성 직할시급 행정구역의 30%이 넘는 인구의 일과 삶에 영향을 준다.

(3) 100만 명 이상의 개인 정보 유출이 발생한다.

(4) 많은 기관, 기업의 민감한 정보가 유출된다.

(5) 대량의 지리, 인구, 자원 등 국가 기본 데이터가 유출된다.

(6) 정부 이미지, 사회 질서 또는 국가 안보를 해치는 심각한 피해를 초래한다.

5. 핵심 정보 인프라로서 인정되는 기타.

핵심 정보 인프라

中倫 ZHONG LUN

3단계 확인

1 핵심 업무 확인

2 중요 업무를 지원하는 정보시스템 또는 산업 제어 시스템 확인

3 핵심업무의 정보시스템 또는 산업 제어 시스템에 대한 의존도 및 정보시스템에 네트워크 보안사고가 발생한 후에 초래할 수 있는 손실에 근거해 핵심 정보 인프라로 확정

B. 플랫폼 류(《국가 네트워크 보안 검사 운영 지침》)

다음 조건 중 하나 충족하면 핵심 정보 인프라로 인정한다.

1. 1천만 명 이상의 등록된 사용자 또는 활성 사용자 (매일 최소 로그인 1회 이상) 수가 1백만 명 이상.
2. 일평균 거래 주문액 또는 거래량이 천만 위안(약 16억 원) 이상.
3. 네트워크 보안 사고가 발생할 경우 다음과 같은 영향이 발생할 수 있다.

(1) 1천만 위안(약 16억 원) 이상의 직접적 경제적 손실을 초래한다.

(2) 1천만 명이 넘는 사람들의 일과 삶에 직접적인 영향을 준다.

(3) 100만 명 이상의 개인 정보 유출이 발생한다.

(4) 많은 기관, 기업의 민감한 정보가 유출된다.

(5) 대량의 지리, 인구, 자원 등 국가 기본 데이터가 유출된다.

(6) 사회적 및 경제적 질서에 심각한 피해를 주거나 국가 안보를 해친다.

4. 핵심 정보 인프라로서 인정되는 기타.

핵심 정보 인프라

中倫 ZHONG LUN

3단계 확인

1 핵심 업무 확인

2 중요 업무를 지원하는 정보시스템 또는 산업 제어 시스템 확인

3 핵심업무의 정보시스템 또는 산업 제어 시스템에 대한 의존도 및 정보시스템에 네트워크 보안사고가 발생한 후에 초래할 수 있는 손실에 근거해 핵심 정보 인프라로 확정

C. 생산 비즈니스 류(《국가 네트워크 보안 검사 운영 지침》)

다음 조건 중 하나 충족하면 핵심 정보 인프라로 인정한다.
1. 성 직할시급 이상 정부기관이 대중에 서비스하는 업무시스템 또는 의료, 보안, 화재, 긴급 명령, 생산 일정, 교통 지휘 등과 관련된 도시 관리 시스템.
2. 1,500개 이상의 표준이 있는 데이터 센터
3. 보안 사고가 발생할 경우 다음과 같은 영향 중 하나가 발생할 수 있다.
(1) 단일 성 직할시급 행정구역의 30%이 넘는 인구의 일과 삶에 영향을 준다.
(2) 10만 명의 물, 전기, 가스, 기름, 난방 또는 교통 외출 등에 영향을 미친다.
(3) 사망자가 5명 이상이거나 심각한 부상자가 50명 이상인 경우.
(4) 5천만 위안(약 82억 원) 이상의 경제적 손실을 직접적으로 초래한다.
(5) 100만 명 이상의 개인 정보 유출이 발생한다.
(6) 많은 기관, 기업의 민감한 정보가 유출된다.
(7) 대량의 지리, 인구, 자원 등 국가 기본 데이터가 유출된다.
(8) 사회적 및 경제적 질서에 심각한 피해를 주거나 국가 안보를 해친다.
4. 핵심 정보 인프라로서 인정되는 기타.

데이터 현지화

제30조 핵심 정보 인프라의 운영자는 중화인민공화국 경내에서 수집 및 생산한 개인 정보와 중요한 데이터를 국내에 저장하여야 한다. 업무적 필요로 해외로 제공해야 하는 경우, 국가 네트워크 부문과 국무원 관련 부서가 함께 제정한 방법에 따라 안전 평가를 진행한다. 법률, 행정 법규에 별도의 규정이 있으면 그 규정을 따른다.

중요 데이터란?

- 업무 데이터와 비즈니스 정보 데이터를 구별할 수 있는가?

안전성 평가의 수행 방법

- 구체적 내용
- 평가 절차

中倫 ZHONG LUN

법률이 규정한 데이터의 국외 전송이란?

- 네트워크를 직접 연결해 데이터를 전송한다.
- 해외 사용자가 데이터를 열람, 획득할 수 있다.
- 국내 데이터가 제 3자에게 전달된 다음 다른 수단을 통해 해외로 전송 또는 휴대한다.
- 데이터 처리를 목적으로 데이터를 해외로 전송한다.

데이터 현지화

기타 관련 규정:

- 신용조회 데이터 (《신용조회사업 관리 규정》제24조)
- 개인 금융 정보 (《은행 금융기관의 개인 금융 정보 보호 작업에 관한 중국인민은행의 통지》제6조)
- 지도 데이터(《지도 관리 조항》제34조)
- 네트워크 출판 서비스에 필요한 기술 장비(《네트워크 출판 서비스 관리 규정》제8조)
- 인터넷 예약 택시 업무 관련 데이터 및 정보 (《인터넷 예약 택시 경영 서비스 관리 임시 방법》27
- 인구 건강 정보 (《인구 건강 정보 관리 방법(시범 운영)》)
- 보험 업무 데이터, 재무 데이터 등 중요한 데이터《보험 회사 개업 검수 지침》

中倫
ZHONG LUN

03 《사이버 보안법》 네트워크 제품 및 서비스 제공업체

中倫律师事务所
ZHONG LUN LAW FIRM

네트워크 제품 및 서비스 제공업체

- 네트워크 제품 및 서비스의 일반적 요구사항 (제22조)
- 네트워크 핵심 설비 및 네트워크 보안 전용제품(제23조)
- 사용자 정보 수집의 법적 요구(제22조)
- 완전한 사용자 정보 보호 제도(제40조)

中倫 ZHONG LUN

기본 요구사항(4가지) :

- 네트워크 제품, 서비스 제공업체는 악성 프로그램을 설치해서는 안 된다.
- 안전 결함, 허점 등 위험성이 있을 때 개선 조치를 취하고, 즉시 사용자와 관련 당국에 보고하여야 한다.
- 보안유지 서비스를 지속적으로 제공하여야 하고, 규정된 기간 혹은 당사자가 약속한 기간 내에는 보안유지 서비스의 제공을 중지해서는 안 된다.
- 네트워크 제품, 서비스가 사용자 정보를 수집할 때, 공급자는 사용자에게 명시하고 동의를 구해야 한다.

中倫
ZHONG LUN

네트워크 핵심 설비 및 네트워크 보안 전용 제품 :

- 자격을 갖춘 기관의 안전 인증 및 안전 테스트를 거쳐야 하고, 관련 국가표준의 강제적 요구사항에 부합하여야 한다.
- 네트워크 핵심 설비 및 네트워크 보안 전용 제품 목록은 국가 네트워크 사무소가 국무원 관련 부서와 함께 제정하고 공포한다.

中倫
ZHONG LUN

04 《사이버 보안법》 관련 법규

中倫律师事务所
ZHONG LUN LAW FIRM

관련 법규

개인 정보 및 중요 데이터 국외 전송 보안 평가 방법(초안)

적용 범위:《사이버 보안법》제37조 규정의 범위를 넘는다. 네트워크 운영자의 데이터 국외 전송은 본 방법을 적용한다. 비 네트워크 운영자(기타 개인 및 조직) 데이터 국외 전송의 보안 평가 업무에 대해서 본 방법을 참고해 집행한다.

'데이터 국외 전송'이란?: 물리적 경계를 넘어 해외의 주체에 데이터를 제공하는 것이다. 즉 데이터 수신자의 출신과 상관없이 데이터의 국외 전송이 이루어지는 것이다. 예를 들면, 국내의 네트워크 운영자가 데이터를 네트워크를 통해 해외의 주체에게 직접 전송하는 것, 해외 주체에게 네트워크를 통한 접근을 허용하고, 국내의 데이터를 열람 및 취득하는 것, 국내의 네트워크 운영자가 네트워크 전송 외 다른 방법(예, 휴대)을 통해 해외의 주체에 제공하는 것이다.

평가 방법: 자체 평가 및 규제기관 평가. 데이터 국외 전송 감독관리의 기본 원칙은 일반 데이터의 경우는 회사(CII 구성여부 상관없이)가 자체 평가를 진행하고, 스스로 책임진다. 특정 데이터의 경우는 규제기관이 평가하고, 국외 전송 허가 여부를 결정한다.

규제기관 : 네트워크 부문은 총괄 조정 역할을 하고, 각 업계 주관 혹은 규제부문의 구체적 조직이 본 업계 내 데이터 국외 전송 보안 평가를 전개한다.

관련 법규

개인 정보 및 중요 데이터 국외 전송 보안 평가 방법(초안)

연례 평가 및 재평가 : 네트워크 운영자는 매년 데이터 국외 전송에 대해 최소 1회 보안 평가를 실시하고, 평가 상황을 업계 관리자 또는 규제 당국에 적시에 보고하여야 한다. 평가 상황이 변경되는 경우, 예를 들면 데이터 수신자가 변경되거나, 데이터 국외 전송 목적, 범위, 수량, 유형 등이 변경되거나, 데이터 수신자 또는 국외 전송 데이터에 중대한 안전사고가 발생될 때 즉시 보안 평가를 재실시하여야 한다. 평가는 단계적으로 이루어져야 한다.

평가 내용 : 첫째, 데이터 국외 전송의 필요성을 입증해야 한다. 평가 과정에서 데이터의 성격과 내용, 데이터의 수량, 수신자 보안 조치, 소재 국가의 법적 환경, 데이터 남용의 위험성 등은 모두 평가 범위에 포함된다.

국외 전송 불가의 상황: 개인 정보가 국외 전송되는 경우에 반드시 정보 주체의 동의를 얻어야 한다. 평가의 절차 요구사항을 충족시키기 위해서 얻은 승인은 반드시 서면으로 작성하고 증명 가능하여야 한다. 국가 안보 및 사회 공공이익에 영향을 미칠 수 있는 데이터 전송은 금지되지만, 평가 방법에서 국가 안보 및 사회적 공익을 해칠 수 있는 특정 상황은 열거하지 않는다. 후속으로 제정하는 국가표준 또는 업계 지침에서 이를 구체적으로 밝혀서 평가 기준으로 삼을 것이다.

개인 정보 및 중요 데이터 국외 전송 보안 평가 방법(초안)

'중요 데이터'란?

《사이버 보안법》이 공포된 후, 제37조가 규정한 중요 데이터의 구체적인 의미와 범위에 대해 많은 논란이 있었다. 입법부는 기업이 법률을 정확히 집행할 수 있도록 후속의 관련 법규를 통해서 이를 명확히 하기를 바란다.

평가 방법의 규정에 따르면, 중요 데이터는 국가 안보, 경제 발전, 사회 및 공공이익과 밀접한 관련이 있는 데이터를 말한다. 구체적인 범위는 국가의 관련 표준 및 중요 데이터 식별 지침을 참고한다. 하지만 이 평가 방법은 여전히 중요 데이터에 대한 명확한 정의가 없고, 후속 제정하는 국가 표준 및 지침에서 이에 대한 운영적 규정을 제공하기를 기대한다.

관련 법규

네트워크 제품 및 서비스 보안 심사 방법(초안)

《사이버 보안법》 제35조에 따라 핵심 정보 인프라 운영자가 구매한 네트워크 제품과 서비스가 국가 안보에 영향을 미칠 수 있다면 국가 네트워크정보부와 국무원 관련 부서가 실시하는 국가 안보 심사를 통과하여야 한다.

행정부서 : 국가 네트워크정보부와 관련 부서는 네트워크 보안 심사위원회를 구성한다.

시행기관 : 네트워크 보안 심사사무실은 네트워크 보안 심사를 구체적으로 마련하고 실시한다.

네트워크 보안 심사위원회는 관련 전문가를 초빙하여 네트워크 보안 심사전문가위원회를 구성하고, 종합적으로 평가한다.

국가가 네트워크 보안 심사 제 3자 기관을 일괄 인증한다. 제 3자 평가 작업

제9조 금융, 통신, 에너지 등 주요 산업의 관할 당국은 국가 네트워크 보안 심사의 요구사항에 따라 본 산업 및 본 분야 네트워크 제품과 서비스의 보안 심사 업무를 실시한다.

관련 법규

네트워크 제품 및 서비스 보안 심사 방법(초안)

심사 범위 :

제2조 국가 안보 및 공공이익과 관련된 정보시스템에 사용되는 중요한 네트워크 제품 및 서비스는 네트워크 보안 심사를 받아야 한다.

제11조 주요 정보 인프라 운영자가 구매한 네트워크 제품 및 서비스는 국가 보안에 영향을 미칠 수 있으므로 네트워크 보안 심사를 받아야 한다.

심사 내용:

제4조, 네트워크 제품 및 서비스의 안전성, 통제가능성을 중점적으로 심사한다.

(1)제품 및 서비스 운영의 불법 통제, 간섭 및 중단 위험성.

(2) 제품 및 주요 구성 요소의 연구개발, 인도 및 기술 지원 과정의 위험성.

(3) 제품 및 서비스 제공자가 제품 및 서비스 제공의 편의를 이용해 사용자 관련 정보를 불법적으로 수집, 저장, 처리 및 활용하는 위험성.

(4) 제품 및 서비스 제공자가 사용자의 신뢰를 이용해 불공정한 경쟁을 실시하거나 사용자 이익을 해치는 위험성.

(5) 국가 안보와 공공이익을 해치는 기타 위험성.

네트워크 제품 및 서비스 보안 심사 방법(초안)

우선 구매 및 블랙리스트 제도:

제10조 정부 부처 및 주요 산업은 심사를 통과한 네트워크 제품 및 서비스를 우선 구매하고, 심사를 통과하지 못한 네트워크 제품 및 서비스를 구매해서는 안 된다.

심사 시작:

제8조 국가의 관련 부서의 요구, 전국업계협회 건의, 시장 반영 및 기업 신청 등에 근거해 네트워크 보안 심사사무실은 제3자 기관, 전문가를 구성해 네트워크 제품 및 서비스에 대해 네트워크 보안 심사를 실시하고, 심사 결과를 게시하거나 특정 범위 내에서 통보한다.

中倫
ZHONG LUN

05 《사이버 보안법》 합법적 경로

中倫律师事务所
ZHONG LUN LAW FIRM

사이버 보안법 위험성

행정 책임

- 정정, 경고, 벌금, 관련 사업 일시 정지 명령, 영업 정지, 사이트 폐쇄, 관련 사업 면허 취소 또는 사업 면허 취소, 직접 책임자에 벌금
- 신용파일에 기록
- 직업 진입 금지

민사 책임

네트워크 운영자가 《사이버 보안법》 위법 행위로 타인에게 손실을 입히는 경우, 해당 행위는 민사 소송 제기가 가능하고, 네트워크 운영자는 이에 상응하는 민사 책임을 져야 한다.

형사 책임

- 《형법 개정안(9)》정보 네트워크 보안 관리 의무의 이행을 거부하고, 네트워크 서비스 제공업체가 법률과 행정 법규가 규정한 정보 네트워크 보안 관리 의무를 이행하지 않고, 규제기관이 명령한 시정 조치를 거부하고, 법률이 규정한 상황에 해당하는 경우 본 죄를 구성한다.
- 《형법 개정안(9)》: 시민 개인 정보를 판매하거나 불법적으로 제공한 죄.

합법적 시행

데이터 합법적 시행 - PMP

私隱管理系統一覽

甲部、基本原則

機構的決心

最高管理層的支持	保障資料主任／部門	匯報
• **私隱管理系統的**成功關鍵，有賴最高管理層的支持，方可有效地推動尊重私隱的文化。	• 有專責人員擔任相關職能，在適當情況下參與機構的決策過程。 • 清晰界定機構內監察循規的角色和責任，並傳達給所有相關人員。 • 負責建立及實施系統監控，持續作出評估及修訂。 • 確保業務中每個涉及使用個人資料的主要部門，均有相應的資料保障政策和程序。	• 建立匯報機制，並在系統監控中反映匯報機制的運作。

系統監控
設立以下監控機制：

個人資料庫存	政策	風險評估工具
• 機構有能力識別其監管或控制的個人資料 • 機構有能力識別其收集、使用及披露個人資料的原因	涵蓋： • 個人資料的收集 • 個人資料的準確性及保留時間 • 個人資料的使用，包括徵求同意方面的規定 • 個人資料的保安 • 機構的個人資料政策及常規的透明度 • 個人資料的查閱及改正	培訓及教育推廣 資料外洩事故的處理 對資料處理者的管理 溝通

乙部、持續評估及修訂

監督及檢討計劃

- 制訂監督及檢討計劃

  保障資料主任／部門應定期制訂監督及檢討計劃，訂出監察及評估系統監控成效的方法。

按需要評估及修訂系統監控

- 更新個人資料庫存
- 修訂政策
- 不斷更新風險評估工具
- 更新培訓及教育的內容
- 訂立資料外洩事故應變機制
- 調整對資料處理者的管理
- 改善溝通

- 사이버 보안 상황의 조사
  - 네트워크 시설 상황
  - 규칙 및 규정
  - 인원 및 자원 배치
  - 합법적 시행 상황
- 인터뷰
- 네트워크 보안 상황의 보고서
- 사이버 보안법 집행에 대한 법률적 제안
- 개선 및 방안 실시
- 교육, 조사 및 검토

中倫
ZHONG LUN

감사합니다

- 중룬 변호사사무소 -