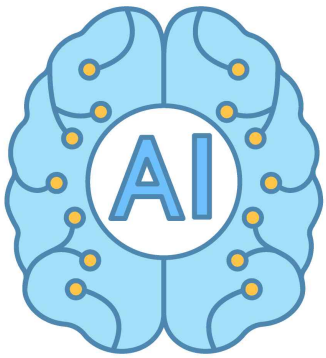
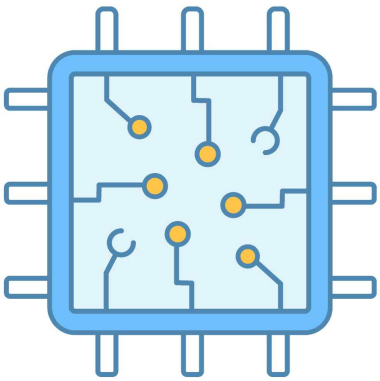
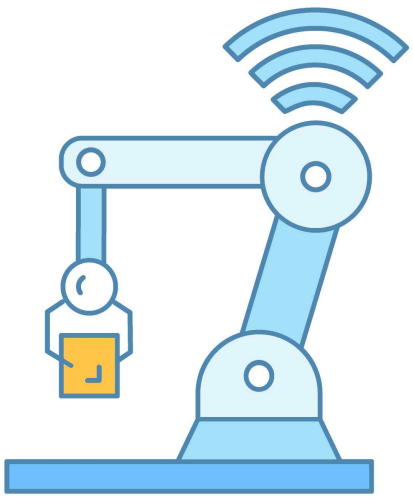
AI/사이버보안 분야

-클라우드 서비스 플랫폼 개인정보보호 요구사항-

플랫폼 개인정보보호 요건에 대한 TBT 관점에서의 검토







산업통상자원부
국가기술표준원

TBT 종합지원센터
R&I Center

이슈 요약

- 커넥트에이아이 최건식 지식재산 최고책임자(CIPO) -

규제 개요

전 세계적으로 'AWS', 'Microsoft Azure', 'Google Cloud Platform(GCP)' 등 주요 글로벌 클라우드 서비스 제공자(Cloud Service Provider, CSP)의 마켓 플레이스 기반의 서비스형 소프트웨어(Software as a Service, SaaS) 유통이 확대됨

이들 플랫폼에 입점하기 위해서는 일정 수준 이상의 보안 및 개인정보 보호 요건을 충족해야 하며, 이는 각국의 개인정보보호법 및 사이버보안법 등 데이터 보호 법률을 플랫폼 정책에 반영되어 있음

유럽(EU), 미국, 싱가포르, 중국은 각기 다른 개인정보보호 규제를 시행하고 있으며, 이를 클라우드 서비스 제공자가 직접 정책에 반영하면서 사적 플랫폼에 의한 기술규제가 형성되고 잇음

국가	데이터 보호 관련 규정
유럽연합	일반 개인정보보호 규정(General Data Protection Regulation, GDPR)
미국	캘리포니아 소비자 개인정보 보호법(California Consumer Privacy Act, CCPA)
싱가포르	개인정보 보호법(Personal Data Protection Act, PDPA)
중국	사이버 보안법, 데이터 안전법
러시아	데이터 현지화법

따라서, 국내 서비스형 소프트웨어(SaaS) 기업이 글로벌 플랫폼에 진출하기 위해서는 사전에 각국의 규제를 검토하여 준수할 필요가 있음

주요 요구사항

주요 클라우드 서비스 제공 플랫폼별 개인정보보호 요구사항은 다음과 같음

주요 플랫폼	데이터 보호 관련 규정
AWS	▪ 유럽연합의 일반 개인정보 보호 규정(GDPR) 대응을 위해, 데이터 처리 계약(Data Processing Agreement, DPA) 제공 필요 ▪ 개인정보 국외 이전 시 표준 계약 조항(Standard Contractual Clauses, SCC) 적용 권고 ▪ 개인정보 처리 방침(Privacy Policy) 링크 필수 제출 필요 ▪ 고객 요청 시 개인정보의 삭제 및 열람 절차 마련 여부 검토 ▪ 아동 온라인 개인정보 보호법(Children's Online Privacy Protection Act, COPPA), 캘리포니아 소비자 개인정보 보호법(CCPA) 등 미국 개인정보 보호법의 준수 여부도 명시 필요
Azure	▪ 이용자 열람·삭제·동의 철회 등 정보 주체 권리 행사 기능을 필수적으로 요구 ▪ 일부 국가에서는 마켓 플레이스 진출기업에 개인정보 영향평가(Personal Information Impact Assessment, PIA) 제출을 요구할 수 있음(Microsoft 진출기업 계약서에 명시)
Google Cloud Platform (GCP)	▪ 사회보장번호, 의료기록 등 민감정보가 포함된 개인식별정보(Personally Identifiable Information, PII) 등록을 제한함 ▪ 미국 건강보험이동성과 책임에 관한 법(Health Insurance Portability and Accountability Act, HIPAA) 적용 대상 솔루션의 경우 사업자 간 계약 체결이 필수적으로 요구됨

산업계 대응방안

클라우드 서비스 제공자 입점 심사에 대비하여, 자체적으로 점검해야 할 기술 및 법률 요건을 사전에 파악하고, 문서화, 인증, 법률 대응 체계의 사전 구축이 필요

목차

1 규제 개요

글로벌 클라우드 서비스 플랫폼의 개인정보 보호 요구사항

개요

전 세계적으로 'AWS', 'Microsoft Azure', 'Google Cloud Platform(GCP)' 등 주요 글로벌 클라우드 서비스 제공자(Cloud Service Provider, 이하 CSP)의 마켓 플레이스 기반 서비스형 소프트웨어(SaaS)* 유통이 확대되고 있으며, 이들 플랫폼에 입점하기 위해서는 일정 수준 이상의 보안 및 개인정보 보호 요건을 충족해야 함

* 서비스형 소프트웨어(Software as a Service, **SaaS**) : 사용자가 소프트웨어를 직접 구매하고 설치하는 대신, 인터넷을 통해 클라우드 환경에서 제공되는 소프트웨어를 사용료를 지불하고 이용하는 방식

해당 요건은 유럽의 GDPR*, 미국 캘리포니아주의 CCPA**, 싱가포르의 PDPA***, 중국의 사이버보안법 등 각국의 데이터 보호 법규를 플랫폼 정책에 반영한 것으로, 국내 SaaS 기업이 글로벌 시장에 진출하기 위해서는 사전에 각국 규제를 충실히 준수할 필요가 있음

* 일반 개인정보 보호 규정(General Data Protection Regulation, **GDPR**)

** 캘리포니아 소비자 개인정보 보호법(California Consumer Privacy Act, **CCPA**)

*** 개인정보 보호법(Personal Data Protection Act, **PDPA**)

무역기술장벽의 연계 구조

글로벌 클라우드 서비스 제공자 플랫폼은 SaaS 제품을 자사 마켓 플레이스에 입점시키기 위해 다음과 같은 보안·프라이버시 기준을 요구함. 이는 이용자 보호와 플랫폼 신뢰도 제고를 위한 것이지만, 실질적으로는 국가별 법령이 민간 플랫폼의 등록 요건화된 것으로, 무역기술장벽(TBT)으로 작용할 수 있음

– 특히 데이터 주권 및 데이터 현지화 정책의 강화는 SaaS 기업에 실질적인 시장 진입 제약으로 작용하고 있음

- 중국, 베트남 등 : 자국 내 수집된 데이터의 해외 이전 제한 및 현지 저장 의무(조건부 이전 가능)
- 러시아 : 모든 개인정보는 반드시 자국 서버에 저장 의무
- 중국 : 핵심 데이터 국외 반출 시 사전심사 요구

주요 국가별 사례

각국의 법령이 클라우드 서비스 제공자의 계약서, 애플리케이션 프로그래밍 인터페이스(API)* 등록 조건, 보안 심사(기초 기술 검토(FTR)** 등)에 구체화 되어 있어 국내 SaaS 기업은 기술적 완성도 외에도 법률·정책 대응 능력을 갖추지 않으면 글로벌 플랫폼 등록조차 어려움

* 애플리케이션 프로그래밍 인터페이스(Application Programming Interface, **API**) : 응용 프로그램에서 사용할 수 있도록, 운영 체제나 프로그래밍 언어가 제공하는 기능을 제어할 수 있게 만든 인터페이스

** 기초 기술 검토(Foundational Technical Review, **FTR**) : AWS 파트너사(특히 SaaS 제공업체 등)가 AWS Marketplace나 Co- sell 프로그램에 참여하기 전에 반드시 거쳐야 하는 보안 및 기술 적합성 심사 절차

[표 1] 주요 국가 사례

국가	대표 법령	클라우드 서비스 제공자 요구사항 반영 사례	비고
유럽연합	일반 개인정보 보호 규정 (GDPR)	▪ DPA* 체결, SCC**적용 ▪ 사용자 동의·삭제권 구현	▪ 'AWS', 'Azure' 모두 적용
미국	캘리포니아 소비자 개인정보 보호법 (CCPA)	▪ 데이터 사용 고지 ▪ 옵트아웃 링크 제공	▪ 일부 클라우드 서비스 제공자는 선택 반영
싱가포르	개인정보 보호법 (PDPA)	▪ 데이터 국외 이전 보호조치, 조직적 보호조치 요구	▪ 'Azure' 싱가포르 지역 중심 적용
중국	사이버 보안법, 데이터 안전법	▪ 데이터 본토 저장 ▪ 핵심 데이터 이전 사전 승인 (조건부 해외 이전 가능)	▪ 'AWS', 'GCP'는 직접 진출 불가
러시아	데이터 현지화법	▪ 러시아 내 저장 의무 ▪ 해외 전송 차단 가능성	▪ 'LinkedIn' 접속 차단 사례 존재

* 데이터 처리 계약(Data Processing Agreement, **DPA**): 데이터 컨트롤러(예: 고객)와 데이터 프로세서(예: SaaS 제공자) 간에 맺는 개인정보 처리에 관한 계약서

** 표준 계약 조항(Standard Contractual Clauses, **SCC**) : EU 외부 국가(예: 한국, 미국)로 개인정보를 전송할 때 적용하는 EU 집행위원회 승인 표준 계약 조항

2 규제 내용

보안·개인정보 보호 요구사항

클라우드 서비스 제공 플랫폼별 보안 요구사항 상세 해설

글로벌 클라우드 서비스 제공자(CSP)는 단순히 제품 등록만을 허용하는 것이 아니라, 사전에 제품이 일정 수준의 보안 기술 요구사항을 충족했는지를 기술 심사를 통해 검토하고 있음

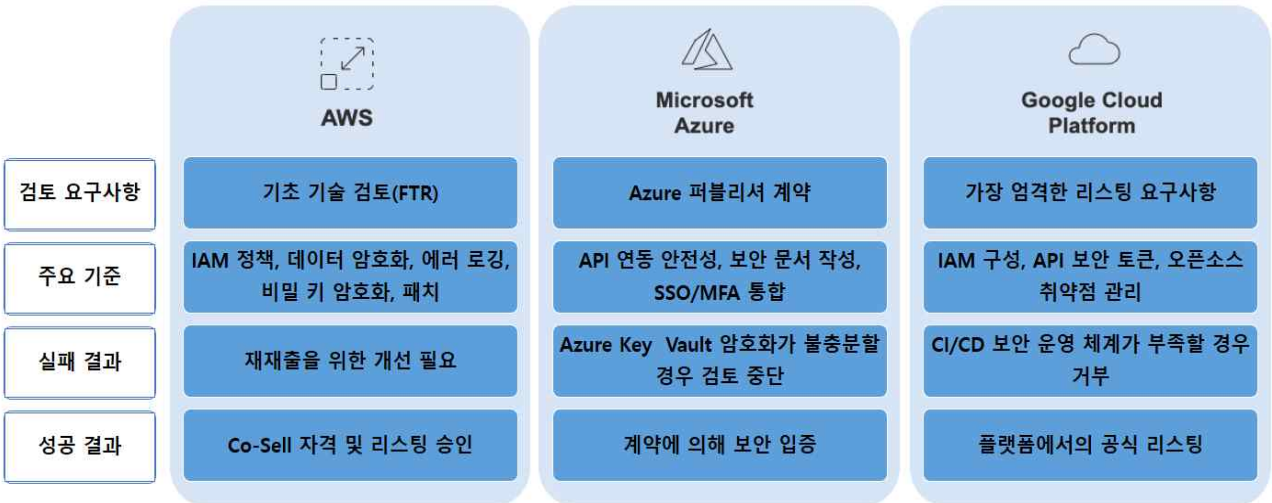
이는 각국의 보안 규제를 사전에 플랫폼 레벨에서 흡수·요건화한 구조이며, 기술·보안 설계 역량뿐만 아니라 국제 기준 기반 대응체계를 갖추어야 한다는 것을 의미함

[표 2] 공통 보안 요건 구조

주요 항목	설명	실제 클라우드 서비스 제공 플랫폼의 요구사항 예시
데이터 암호화	▪ 저장/전송 구간 데이터 모두 암호화 필요 ▪ 암호화 방식 : AES-256*, TLS 1.2** 이상 필수 * AES-256 : 데이터 자체를 암호화하는 알고리즘으로, 저장 데이터를 보호하는 데 사용됨 ** TLS 1.2 : 고객과 서버간의 통신을 암호화하는 보안 규칙	▪ AWS FTR 암호화 요구 ▪ 'Azure Key Vault'(암호화 키) 권장 ▪ 'GCP' 보안 프로토콜 요구
접근 권한 통제 (IAM)	▪ 사용자·관리자 권한 분리, 역할 기반 접근통제 (Role-based Access Control) 구현	▪ IAM* 정책 구성 오류 시 심사 반려 사례 다수 * 사용자 인증 및 권한 관리 기능(Identity and Access Management, **IAM**)
취약점 관리	▪ OWASP* 기준 취약점 제거, 악성코드 제거, 정기 스캔 필요 * 전 세계적으로 가장 권위 있는 웹 보안 가이드라인을 제시하는 비영리 단체 (Open Web Application Security Project, **OWASP**)	▪ AWS AMI 이미지 제출 시 자동 검사
백도어·보안 위협 방지	▪ 백도어, 숨겨진 명령어, 원격제어 코드 삽입 금지	▪ 'Azure Marketplace' 등록 심사 거부 사유 중 다수 발생
시스템 모니터링	▪ CPU·메모리·로그 이상 탐지 기능 요구 (CloudWatch 등 연동)	▪ 미국 공인회계사협회의 신뢰 서비스 기준(SOC 2) 감사기준에 필수 요소
보안 인증(외부)	▪ 정보보안경영시스템(ISO/IEC 27001) ▪ 미국 공인회계사협회의 신뢰 서비스 기준(SOC 2)* ▪ 클라우드 서비스를 위한 ISO/IEC 27002 기반 정보보안 통제를 위한 실무 규정(ISO/IEC 27017) 등 * 미국 공인회계사협회의 신뢰 서비스 기준(Service Organization Control 2, **SOC 2**) : 클라우드·IT 서비스를 제공하는 조직이 데이터보안, 가용성, 기밀성 등을 얼마나 잘 관리하는지를 제3자가 감사를 통해 평가	▪ AWS Marketplace **Vendor Insights***, GCP Trust Center**에서 반영 * 보안과 관련된 정보 및 법적·제도적 준수 여부를 하나의 통합 화면에 모아 보여줌으로써, 제3자 소프트웨어의 위험 평가를 보다 쉽게 할 수 있도록 도와주는 서비스 ** Google Cloud Platform Trust Center는 클라우드의 위치를 확보하기 위해 보안, 규정준수, 개인정보 보호에 주력하는 보안 서비스

[표 3] 주요 CSP 별 세부 보안 심사 내용

클라우드 서비스 제공 플랫폼	세부 보안 심사
AWS	▪ 마켓 플레이스 입점 필수 단계 ▪ 주요 심사 항목 : IAM 정책, 데이터 암호화 여부, 에러 로깅 구조, 보안 비밀키 암호화, 패치 체계 등 ▪ 통과 시 Co-Sell 자격* + 리스팅 승인(Listing Approval)**, 미통과 시: 개선 요구 후 재제출 * AWS와 입점 기업(판매자)이 공동으로 제품을 판매하는 자격 ** AWS 마켓플레이스에 상품(소프트웨어 등)을 정식으로 출시할 수 있는 최종 승인
Microsoft Azure	▪ Azure Publisher Agreement에 따라 모든 SaaS는 보안성 입증이 필요 ▪ API 연동 안정성, 보안 문서 작성 여부, SSO* 및 MFA** 통합 여부가 주요 심사기준 ▪ Microsoft Azure에서 제공하는 클라우드 보안 키 관리 서비스(Azure Key Vault) 기반 암호화 구성 미비 시, 심사 중단 사례 다수 * 단일 로그인(Single Sign-on, **SSO**) : 한 번 로그인으로 여러 애플리케이션이나 서비스에 자동으로 인증되는 기능 ** 다중 인증 요소(Multi- Factor Authentication, **MFA**) : 2개 이상의 인증 수단을 요구하여 로그인 보안을 강화하는 방식(비밀번호 외에 OTP, 인증앱, 생체인식 등을 추가로 요구)
Google Cloud Platform	▪ GCP는 플랫폼 내 정식 리스팅 요건이 가장 엄격한 편으로, IAM 구성, API 보안 토큰 방식, 오픈 소스 취약점 관리 도구 적용 여부 등을 중점 확인 ▪ CI/CD* 과정에 보안 운영 체계가 없다면, 입점 자체를 반려하는 사례도 존재 * 지속적 통합(Continuous Integration, **CI**) : 개발 중인 소프트웨어를 정기적으로 주 저장소에 통합하는 과정 지속적 개발(Continuous Deployment, **CD**) : 개발된 소프트웨어를 자동으로 테스팅하고 프로덕션 환경으로 배포하는 과정. 지속적 통합(CI)과 연계됨



[그림 1] 클라우드 서비스 제공 플랫폼 보안 검토 비교

개인정보보호 요건과 국가별 법령 연계 구조

글로벌 클라우드 서비스 제공 플랫폼들은 서비스형 소프트웨어(SaaS) 제품을 등록하고 유료 서비스로 운영하려는 기업에 다양한 개인정보 보호 준칙을 요구하고 있음

이는 단순히 '프라이버시 정책을 작성하라'는 수준을 넘어서, 실제 국가별 법령을 준수할 수 있는 구조와 프로세스를 갖췄는지를 요구하는 구조로 진화하고 있음

특히 유럽(EU), 미국, 싱가포르, 중국은 각기 다른 개인정보보호 규제를 시행하고 있으며, 이를 클라우드 서비스 제공자가 직접 정책에 반영하면서 사적 플랫폼에 의한 비공식 기술규제가 형성되는 양상임

[표 4] 주요 국가별 법령 요건 비교

국가	대표 법령	핵심 조항 및 요건
유럽연합	일반 개인정보보호 규정(GDPR) (EU 2016/679)	▪ 제5조 개인 데이터 처리 관련 원칙 ▪ 제6조 처리의 합법성 ▪ 제7조 동의 요건 ▪ 제30조 개인정보 처리 기록 유지 ▪ 제44조 이전에 대한 일반 원칙
미국 (캘리포니아)	소비자 개인정보보호법(CCPA)	▪ 1798.100 개인정보 수집 기업의 일반 의무 ▪ 1798.120 개인정보 파냄 또는 공유 거부(옵트아웃)* 권리 * 소비자가 자신의 개인정보를 제3자에게 판매하지 못하도록 거부할 수 있는 권리
싱가포르	개인정보보호법(PDPA)	▪ 제13조 동의 필수 ▪ 제26조 국외 개인정보 이전
중국	사이버 보안법	▪ 제37조 국외 이전 사전심사, 중요정보 본토 저장 의무

❖ 국가별 법령 관련 조항 세부내용

1) EU, 「일반 개인정보보호법(GDPR)」

- **(제5조, 개인 데이터 처리 관련 원칙)**
  명시적이며 정당한 목적을 위해 수집되어야 하며, 그 목적과 양립할 수 없는 방식으로 추가 처리되어서는 안 됨. 다만, 공익적 보관 목적, 과학적 또는 역사적 연구 목적, 통계 목적을 위한 추가 처리는 제89조 제1항에 따라 최초 목적과 양립할 수 없는 것으로 간주되지 않음 (목적 제한 원칙)

- **(제6조, 처리의 합법성)**
  개인정보 처리는 다음 중 최소 하나 이상의 조건에 해당하는 경우에만 적법한 것으로 간주됨
  - 정보 주체가 하나 이상의 특정한 목적을 위해 자신의 개인정보 처리에 동의한 경우
  - 정보 주체가 당사자인 계약을 이행하기 위해, 또는 계약 체결 이전에 정보 주체의 요청에 따라 필요한 조치를 취하기 위해 처리가 필요한 경우
  - 개인정보처리자가 법적 의무를 준수하기 위해 처리가 필요한 경우
  - 정보 주체 또는 다른 자연인의 중대한 이익(생명·신체 등)을 보호하기 위해 처리가 필요한 경우
  - 공익을 위한 업무 수행 또는 개인정보처리자에게 부여된 공권력 행사를 위해 처리가 필요한 경우

- 개인정보처리자 또는 제3자가 추구하는 정당한 이익을 위해 처리가 필요한 경우(단, 이러한 이익보다 정보 주체의 이익, 기본권 및 자유, 특히 정보 주체가 아동인 경우는 우선 보호되어야 함)

- **(제7조, 동의 요건)**
  개인정보 처리가 정보 주체의 동의를 기반으로 하는 경우, 개인정보처리자는 정보 주체가 개인정보 처리에 동의했음을 입증할 수 있어야 함

- **(제30조, 개인정보 처리 기록 유지)**
  각 개인정보처리자 및 해당되는 경우 개인정보처리자의 대표자는, 자신의 책임 하에 수행되는 개인정보 처리 활동에 대한 기록을 유지해야 함. 해당 기록에는 다음의 모든 정보가 포함되어야 함
  - 개인정보처리자 및, 해당되는 경우 공동 개인정보처리자, 개인정보처리자의 대표자, 개인정보 보호책임자(DPO)의 이름과 연락처
  - 개인정보 처리의 목적
  - 정보 주체의 범주 및 개인정보의 범주에 대한 설명
  - 개인정보가 제공되었거나 제공될 수신자 범주(제3국 또는 국제기구 수신자 포함)
  - 해당되는 경우, 개인정보가 이전되는 제3국 또는 국제기구의 명칭,
  - 그리고 GDPR 제49조 제1항 2문단에 따른 이전의 경우에는 적절한 보호조치에 대한 문서화
  - 가능한 경우, 각 개인정보 범주별 삭제 예정 시한
  - 가능한 경우, GDPR 제32조 제1항에 언급된 기술적 및 조직적 보안 조치에 대한 일반적인 설명

- **(제44조, 이전에 대한 일반 원칙)**
  처리 중이거나, 이전 후 처리를 목적으로 하는 개인정보의 제3국 또는 국제기구로의 이전은, 이 규정의 다른 조항들을 준수하는 것을 전제로 하여, 이 장(국외 이전 관련 조항)에서 정한 조건을 개인정보처리자 및 수탁자가 모두 준수하는 경우에만 허용됨. 이는 제3국이나 국제기구로부터 다른 제3국 또는 국제기구로 개인정보가 재이전되는 경우에도 적용됨

2) 미국 캘리포니아,「소비자 개인정보보호법(CCPA)」

- **(1798.100, 개인정보 수집 기업의 일반 의무)**
  개인정보를 수집하고 이를 제3자에게 판매 또는 공유하거나, 서비스 제공자(service provider) 또는 계약자(contractor)에게 업무 목적으로 제공하는 기업은 다음 요건을 포함한 계약을 체결해야 함
  - 해당 개인정보는 기업이 지정한 제한된 목적을 위해서만 판매 또는 제공된다는 점 명시
  - 제3자·서비스 제공자·계약자가 본 법률에 따른 의무를 이행하고 동일 수준의 개인정보 보호 조치를 제공하도록 요구
  - 개인정보가 본 법의 요구사항에 맞게 사용되도록, 기업이 점검·감독할 수 있는 권리 보장
  - 제3자 등이 더 이상 법적 의무를 이행할 수 없다고 판단한 경우, 기업에 통지할 의무 부여
  - 위와 같은 통지를 포함하여 기업은 무단 사용을 중단하고 시정 조치를 취할 수 있는 권리를 가짐

- **(1798.120, 개인정보 판매 또는 공유 거부 권리)**
  소비자는 언제든지, 자신의 개인정보를 제3자에게 판매하거나 공유하는 기업에 대해, 자신의 개인정보를 판매 또는 공유하지 말도록 요청할 권리를 가짐. 이 권리는 "판매 또는 공유 거부권(opt-out right)"이라 불릴 수 있음

3) 싱가포르, 개인정보보호법(PDPA)

- **(제13조, 동의 필수)** 다음의 경우가 아니면 개인에 관한 개인정보를 수집, 이용 또는 공개해서는 안 됨
  - 해당 개인이 본 법상 정보의 수집, 이용 또는 경우에 따라 공개에 대한 동의를 하거나 동의를 한 것으로 간주되는 경우
  - 본 법 또는 기타 법률에 따라 개인의 동의 없이도 수집, 이용 또는 공개(경우에 따라)가 필요하거나 승인된 경우

- **(제26조, 국외 개인정보 이전)**
  (1) 조직은 본 법에 따라 이전된 개인정보에 대해 본 법에 따른 보호수준에 상응하는 표준 개인정보 보호 수준을 제공하도록 본 법에 명시한 요건에 따른 경우를 제외하고는 싱가포르 외부의 국가나 영토로 개인정보를 이전해서는 안 됨
  (2) 위원회는 조직의 신청이 있을 시 서면 통지로 해당 조직의 개인정보 이전과 관련하여 (1)항에 따라 명시된 요건을 면제할 수 있음
  (3) (2)항에 따른 면제는 (a) 위원회가 서면으로 명시할 수도 있는 조건에 따라 부여될 수 있으며, (b) 관보에 게재될 필요가 없고 위원회가 언제라도 취소할 수 있음
  (4) 위원회는 본 조항에 부과된 조건을 언제든지 추가, 변경 또는 철회할 수 있음

4) 중국,「사이버보안법」

- **(제37조, 국외 이전 사전심사, 중요정보 본토 저장 의무)**
  중요정보기반시설 운영자는 중국 국내에서 수집하거나 생성한 개인정보 및 중요 데이터를 반드시 중국 내에 저장해야 하며, 업무상 국외로 제공이 반드시 필요한 경우, 국가인터넷정보판공실 등 관계 부처가 정한 절차에 따라 보안 심사(사전심사)를 거쳐야 함

– CSP 별 개인정보 요건과 법령 반영 구조는 다음과 같음

1) AWS

- AWS는 유럽연합의 일반 개인정보 보호 규정(GDPR) 대응을 위해 데이터 처리자 계약(Data Processing Agreement, DPA)을 제공
- 개인정보 국외 이전 시 표준계약조항(Standard Contractual Clauses, SCC)의 적용을 권고
- 출품사는 개인정보 처리 방침(Privacy Policy) 링크를 필수로 제출해야 함
- 고객 요청 시 개인정보의 삭제 및 열람 절차 마련 여부도 검토 대상
- 이와 함께 아동 온라인 개인정보 보호법(Children's Online Privacy Protection Act, COPPA), 캘리포니아 소비자 개인정보 보호법(California Consumer Privacy Act, CCPA) 등 미국 개인정보 보호법의 준수 여부도 명시

2) Azure

- Azure는 Market Place 진출 기업과 Microsoft 간의 법적 책임 구분(데이터 통제자 간 계약)을 명확히 함
- 개인정보 처리 방침 제공은 물론, 이용자의 열람·삭제·동의 철회 등 정보 주체 권리(Data Subject Rights) 행사 기능을 필수 요구

- 일부 국가에서는 진출 기업에 개인정보 영향평가(Personal Information Impact Assessment, PIA) 제출을 요구할 수 있으며, 이러한 조건은 Microsoft 진출 기업 계약서(Microsoft Publisher Agreement) 8.0에 명시됨

3) Google Cloud Platform(GCP)

- GCP는 개인식별정보(Personally Identifiable Information, PII), 특히 사회보장번호, 의료기록 등 민감정보가 포함된 콘텐츠의 등록을 제한함
- 미국 건강보험이동성과 책임에 관한 법(Health Insurance Portability and Accountability Act, HIPAA) 적용 대상 솔루션의 경우 사업자 간 계약(Business Associate Agreement, BAA)체결 필수

[표 5] CSP 별 보안 요건

항목	AWS	Azure	GCP
개인정보 처리 방침 제출	필수	필수	필수
GDPR 준수 문서 (DPA 등)	제출 권장	계약서 내 명시적 구조	일부 서비스에 필수 적용
사용자 권리 보장 (열람·삭제)	구현 권고	구현 필수	필수 (특히 EU 대상)
국외 이전 통지·동의 절차	SCC 또는 계약 기반 처리	SCC 또는 Privacy 항목 기반	위치 기반 지역(region) 선택 정책* 제공 * 사용자의 위치나 법적 요구사항을 고려해, 데이터를 저장할 지역을 자동으로 정해주는 정책
법적 책임 구조	독립 컨트롤러 선언	진출 기업 중심, MS는 중개자	GCP는 공동 책임 포함 가능

CSP 기술 심사 절차와 입점 시나리오

CSP 플랫폼에 SaaS 제품을 등록하기 위해서는 단순한 양식 등록을 넘어 사전 보안 심사와 기술 구조 검증 절차를 통과해야 함

이를 통해 각 CSP는 자사 마켓 플레이스를 통해 유통되는 제품의 보안성, 안정성, 법적 준수 수준을 확보함

[표 6] CSP 별 기술심사 절차 개요

CSP	주요 사전 심사 프로그램	필수 여부	심사 항목 예시
AWS	▪ 기초 기술 검토 (Foundational Technical Review, **FTR**)	필수	▪ IAM 구성 ▪ 암호화 구현 ▪ 보안 패치 체계 ▪ 로깅 구조 등

Azure	▪ Azure 인증 ▪ 기술 요건 확인서(Technical Questionnaire)	필수	▪ Microsoft Entra ID* 연동 ▪ API 연동 체계 ▪ 약관/개인정보 처리 방침 등록 등 * 제로 트러스트 액세스 제어를 설정하고, ID 공격을 방지하고, 리소스에 대한 액세스를 관리
GCP	▪ Google Marketplace 등록 심사 (Listing Review) ▪ 제품 평가(Product Assessment)	필수	▪ IAM 구성 ▪ 개인식별정보(PII) 필터링 ▪ GCP 리전 저장 여부 ▪ 서비스 수준 계약(SLA 문서)* 제출 등 * 서비스 수준 계약(Service Level Agreement, **SLA**) : 서비스 제공자(SaaS 기업)와 이용자(고객 또는 플랫폼) 간에 서비스의 가용성, 응답시간, 지원 수준 등을 명시적으로 약속한 서비스 수준 계약서

[그림 2] SaaS 제품의 CSP 입점 기술 심사 절차 흐름

실제 기업 사례를 통해 본 CSP 요구사항

CSP의 기술 심사 및 개인정보 요구사항은 규제 준수 관점에서 명확한 기준이 없거나, 기업 입장에서 실현 가능성이 낮을 경우 실질적인 무역기술장벽으로 작용하게 됨

특히 중소 SaaS 기업은 인력, 예산, 문서 역량의 한계로 인해 플랫폼 입점 자체가 지연되거나 중단되는 경우가 많으며, 일부는 고객 요구에도 불구하고 글로벌 판매 기회를 포기하기도 함

[표 7] 주요 문제 원인과 영향분석

유형	문제 원인	결과 및 영향
기술 인증 부족	▪ ISO/IEC 27001, SOC 2, ISO/IEC 27017 등 인증 미비	▪ 보안 심사 미통과, 일정 지연
민감정보 정책 불일치	▪ CSP의 개인식별정보(PII) 차단 정책과 기업 서비스 구조 불일치	▪ 제품이나 서비스 등록 반려, 구조 변경 필요
국가 법령 충돌	▪ CSP 입점 승인 ≠ 현지 규제 통과	▪ 판매 제한, 이중 규제 발생

– 실제 기업의 수출 애로사항은 다음과 같음

사례 1. [A사] ISO 인증 미보유로 AWS 입점 심사 지연

기업 개요	국내 Business to Business(B2B) 인사관리 SaaS 서비스 운영
목표시장	북미 (AWS Marketplace 공동영업 프로그램 연계 계획)
문제 발생	▪ ISO/IEC 27001 및 SOC 2 인증 미보유 → FTR 심사 중 보안 통제 항목에서 '정량적 증빙 없음' 판정 ▪ IAM 구성은 있었으나 문서화·재현성 미흡 → 기술 아키텍처 재구성 요청
결과	▪ 심사 지연 5주 ▪ 고객 공동 영업 기회(PoC* 등) 누락, 개발팀 인력 추가 투입으로 일정 차질 ▪ 향후 SOC 2 감사보고서 획득을 위한 예산 필요성 인식 * 개념 증명(Proof of Concept, **PoC**) : 제품, 기술, 정보 시스템 등이 조직의 특수 문제 해결을 실현할 수 있다는 증명 과정을 의미함. 아직 시장에 나오지 않은 신제품에 대한 사전 검증을 위해 사용됨

사례 2. [B사] GCP 입점 과정에서 민감정보 필터링 실패

기업 개요	이미지 기반 의료 AI 분석 SaaS (피부병 판독 API 제공)
문제 발생	▪ API 입력값 중 일부가 주민등록번호 형식(PIN) 또는 의료기록 일부를 포함 ▪ GCP 정책상 "개인식별정보(PII) 포함 여부 자동 스캔 + 거부" 기능에 의해 리스팅 자체 불가

	▪ Google Trust & Safety 팀에서 수작업 심사 요청
대응	▪ 민감정보 필터링 로직 수정 ▪ 입력값에 대한 "비식별 처리 로직 삽입" + 사용자 동의 강화 ▪ 유럽의 일반 개인정보보호법(GDPR)에 따른 데이터 처리 계약(DPA) 작성 및 개인식별정보(PII) 예외 항목 표기
결과	▪ 리스팅 완료까지 총 9주 소요 ▪ 의료정보 관리 역량이 부족했다면 시장 진입 자체가 불가능했을 상황

사례 3. [C사] 중국 진출 시 CSP 요건 외 국가 규제 중복 발생

기업 개요	교육용 SaaS 솔루션
문제 발생	▪ 중국 로컬 CSP(Alibaba Cloud) 입점은 통과했지만, 중국 사이버 보안법상 "국내 사용자 데이터는 반드시 중국 내 저장" 요건 존재 ▪ 중국의 정보보안 등급 보호제도(Multi-Level Protection Scheme, MLPS) 2.0 인증 미보유 → 교육부 대상 판매 제한
결과	▪ CSP 기술심사는 통과했지만, 법령상 현지 저장 인프라·규제 인증 미비로 거래 불가 ▪ CSP 입점이 무역장벽을 완화하지 못하고, 현지 법령이 추가적 TBT로 작용한 사례

주요 문제 원인과 그 영향을 분석해보면 CSP 심사 자체도 높지만, CSP와 현지 법령의 이중 대응이 필요한 현실 속에 글로벌 진출을 위해서는 기술개발뿐 아니라 법제 모니터링, 인증 전략, 구조 설계 내재화가 병행되어야 함

CSP 요구사항과 국제표준

글로벌 CSP가 요구하는 보안·개인정보 보호 요건은 명시적으로는 각국의 법령에 기반하지만, 실무적으로는 국제표준(ISO/IEC, AICPA 전문 표준* 등)의 프레임워크를 참조하여 심사기준을 설정하고 있음. 그러나 일부 항목에서는 표준 요구와 CSP 자체 기준 간 불일치가 발생하며, 국내 기업은 이에 따라 중복 대응 비용과 해석상의 혼란을 겪고 있음

- CSP는 보안·개인정보 요구사항의 설계 기준으로 ISO/SOC 등을 활용하지만, 실제 심사에서는 자사 요구사항을 '절대 기준'으로 적용함
- 국제 인증을 받아도 CSP 심사에서 보완을 요구받는 경우 많아 기업의 입장에서 인증은 "면책"이 아니라 "입증자료"로 간주됨

* 미국 공인회계사협회(American Institute of Certified Public Accountants, AICPA)가 개발, 발행 및 시행하는 표준(감사 및 보증 표준, 세무 표준 등)

[표 8] 국제표준별 CSP 적용

표준 번호	개요	CSP 적용 형태
ISO/IEC 27001	◆ 정보보호 관리체계(ISMS) 국제표준	▪ AWS, Azure, GCP에서 권장, ▪ 판매자(Vendor)가 자신의 SaaS 제품을 Vendor Insights에 등록하기 위해 해당 표준을 충족해야 함
ISO/IEC 27017	◆ 클라우드 서비스 보안 가이드라인	▪ 일부 CSP는 요구사항 참조 수준, Azure Cloud Security 기본 프레임워크 반영
ISO/IEC 27701	◆ 개인정보보호 관리체계 확장 표준 (GDPR 대응)	▪ GDPR 대상 서비스 운영 시 CSP에서 DPA 요구와 함께 권장
SOC 2 (Type I/II)	◆ AICPA 기준 신뢰서비스 통제(보안, 가용성 등) 보고서	▪ AWS Co-Sell, GCP 고위험 서비스 등록 시 핵심 인증 자료로 간주
CSA STAR	◆ 클라우드 보안 협회(Cloud Security Alliance)의 CSP 보안 평가 프레임워크	▪ 일부 CSP는 Vendor 평가 참고용으로 활용, 강제성은 없음

표준명	주요 내용 요약	CSP 적용 형태 요약
ISO/IEC 27001	◆ 정보보호 관리체계(ISMS) 국제표준. 정책·위험·운영·모니터링 포함	◆ AWS Vendor Insights, Azure 보안 문서로 활용
SOC 2 (Type II)	◆ 보안·가용성·기밀성* 등 5대 신뢰원칙 기반 제3자 감사제도 * (예시 설명) **보안**: 시스템 무단 접근, 사용, 변경, 손상 보호, **가용성**: 계약수준에 따른 서비스 지속 사용 **기밀성**: 비인가인에게 정보 노출 보호	◆ CSP 심사 시 감사보고서 제출 요구 (AWS/GCP)
ISO/IEC 27701	◆ 개인정보보호 관리체계(PIMS). GDPR 대응에 유리	◆ CSP의 DPA 계약 요구 및 SCC 요건 간소화 근거
ISO/IEC 27017/27018	◆ 클라우드 보안/프라이버시 가이드라인	◆ 일부 CSP 정책(예: GCP)에서 기술 기준 참조
CSA STAR	◆ 클라우드 보안 인증, CCM 기반 자율 공개체계	◆ CSP는 신뢰 프레임워크로 활용하되 필수는 아님

CSP에서 요구하는 등록 문서들은 각국의 법적 요건과 연결되어 있으며, 글로벌 SaaS 제공자는 다음 문서들을 플랫폼 기준에 맞춰 번역·재구성해야 함

[표 9] CSP 등록 문서 관련 근거 법령

문서 구분	목적 / 적용 법령	CSP 적용 방식
서비스 수준 협약 (Service Level Agreement, SLA)	▪ 서비스 수준 협약, 가용성/장애 처리 등 약속	▪ 등록 시 필수, 일부 CSP는 샘플 템플릿 제공
서면 계약 (Data Processing Agreement, DPA)	▪ 개인정보 처리자 (GDPR 제28조)	▪ AWS/Azure: 표준 DPA 체결 요구
표준 계약 조항 (Standard Contractual Clauses, SCC)	▪ 보호조치를 조건으로 한 이전 (GDPR 제46조)	▪ EU 대상 서비스 시 CSP가 권고 또는 계약 포함
개인정보 영향평가 (Privacy Impact Assessment, PIA)	▪ 개인정보 영향평가 (PDPA, GDPR 기반)	▪ 일부 CSP(GCP 등)는 제출 요구 가능
개인정보 처리 방침	▪ 데이터 수집·처리 방침 공개용	▪ 모든 CSP에서 영문 문서 필수 업로드 항목

❖ **EU, 「일반 개인정보보호법(GDPR)」**

- **(제28조, 개인정보 처리자)** 개인정보 처리는 **개인정보처리자와 처리자 간의 계약(Data Processing Agreement)** 또는 EU 또는 회원국 법에 따른 다른 법적 행위에 따라 이루어져야 하며, 해당 계약 또는 법적 문서는 다음 사항을 명시해야 함
  - 처리의 주제와 기간
  - 처리의 성격과 목적
  - 처리되는 개인정보의 종류 및 정보 주체의 범주
  - 개인정보처리자의 의무 및 권리
- **(제46조, 적절한 보호조치를 조건으로 한 이전)** 적절한 보호조치는, 감독기관의 별도 승인이 없이 다음을 통해 제공될 수 있음
  - 공공기관 간 법적 구속력이 있고 집행 가능한 문서
  - 제47조에 따른 구속력 있는 기업 내부 규칙(Binding Corporate Rules, BCR)
  - 제93조 제2항의 심사 절차에 따라 위원회가 채택한 **표준 개인정보 보호 조항**
  - 감독기관이 채택하고 위원회가 승인한 **표준 개인정보 보호 조항**
  - 제40조에 따른 승인된 행동강령(Code of Conduct)
  - 제3국 내 개인정보처리자 또는 처리자가 해당 보호조치를 준수하겠다는 법적 구속력 있고 집행 가능한 약속
  - 제42조에 따른 승인된 인증 메커니즘(Certification Mechanism)
  - 제3국 내 개인정보처리자 또는 처리자가 보호조치를 이행하겠다는 법적 구속력 있는 약속

3 시사점 및 산업계 대응방안

시사점

규제 요건과 대응 간극

글로벌 CSP 마켓 플레이스 입점 과정에서 국내 서비스형 소프트웨어(SaaS) 기업들은 제품 자체의 우수성과는 별개로, 다음과 같은 진입장벽에 직면하고 있음

보안·개인정보 보호 요건이 CSP 정책에 통합되면서, '보안 내재화', '문서화 역량', '법적 이해력'이 부족할 경우 입점 자체가 어렵거나 지연되는 사례가 다수 발생함

[표 10] 주요 문제 사례

분류	주요 문제
인증 역량 부족	ISO/IEC 27001, SOC 2 인증 미보유 → 심사 지연, 고객사 신뢰도 저하
보안설계 미흡	IAM 역할 분리, 데이터 암호화 등 보안 구조 미 정립 상태에서 기술 심사 탈락
문서 작성 미비	SLA, 개인정보 처리 방침, DPA 등 필수 문서 미흡 또는 번역 부족
법령 해석 어려움	국가별 개인정보 보호법(GDPR, PDPA, CCPA 등) 국가별 요건의 CSP 반영 내용 해석 곤란
대응 리소스 부족	중소 SaaS 기업의 경우 전담 개발자·보안 인력 없이 설계·심사·문서화 동시 대응 불가능

해외 주요국의 산업계 반응 및 중소기업 지원 전략

글로벌 CSP 요건은 해당 플랫폼이 위치한 국가의 정책 환경과도 밀접하게 연계되어 있음. 각국은 자국 기업 보호, 자율규제 확대 또는 혁신 보전 등을 명분으로 CSP 규제 요건을 수용하거나 해석하고 있으며, 산업계와 중소기업을 위한 대응도 다르게 전개됨

[표 11] 국가별 산업계 반응

국가	산업계 반응 요약	정책적 흐름 및 특징
EU	▪ CSP 규제가 GDPR 등과 연계됨에 따라 법적 확실성 확보는 긍정적 ▪ 중소기업에 행정적 부담 우려	▪ 유럽 집행위원회 및 스타트업 기업 대상 규제 완화 의견 수렴 (2025.4)
미국	▪ 미국 국립표준기술연구소 위험관리 프레임워크, 인공지능 권리장전(AI Bill of Rights) 가이드라인 제시	▪ 미국 국립표준기술연구소의 AI 위험관리 프레임워크(AI RMF)와 백악관 과학기술정책실의 AI 권리장전(AI Bill of Rights)은 법적 구속력이 없는 자율 가이드라인으로, 기업의 신뢰성 확보와 공정한 알고리즘 설계에 대한 권고 수준에서 활용되고 있음
영국	▪ 산업별 규제 자율성 확보에 집중 ▪ CSP 요건보다 공공부문 입찰 시 AI 윤리 요건 강조	▪ 비강제성 규범적 접근 선호
싱가포르	▪ 싱가포르의 인공지능 자율 인증(AI Verify)을 통해 중소기업의 부담 완화	▪ 설명 가능성·리스크 관리 중심의 자율 인증체계 운영 중
일본	▪ 공공 조달에 CSP와 ISO 기반 윤리 가이드라인 요구 확대	▪ 정보기술 인공지능 위험관리 가이드 (ISO/IEC 23894) 기반 시스템 구축 시 가점 부여

- EU 집행위원회는 인공지능법(AI Act) 및 일반 개인정보보호법(GDPR)을 준수하기 위해 과도한 부담을 겪고 있는 중소기업을 위해 플랫폼 등록 절차, 문서 작성, 샌드박스 심사기준 등을 완화할 수 있도록 의견 수렴 중

[표 12] 주요국별 중소기업 지원 정책

구분	정책명/프레임워크	SME 지원방식	특징
EU	Digital SME Initiative	규제 샌드박스, 공동 인증 시범	AI Act 의견 수렴 포함
싱가포르	AI Verify	리스크 관리 중심 인증 우대	CSP 요건 기반 인증 자동화
미국	NIST Cybersecurity Framework	자율 가이드라인 제공	CSP 별 보안 기준과의 호환성 우수
일본	공공조달 AI 윤리 기준	ISO 표준(ISO/IEC 27001 등) 충족 시 가점 부여	CSP 기준과 공공 조달 정책 연결
한국	KISA 글로벌 진출 지원사업	GDPR 대응 컨설팅, ISO 인증 비용 보조	CSP 대응 인프라 미비로 대응 확대 필요

TBT 해석 관점

CSP의 보안 및 개인정보 보호 요구사항은 자율적 기술규정처럼 보이지만, 다음과 같은 요소들로 인해 WTO TBT 협정의 주요 원칙에 저촉될 가능성이 존재함

[표 13] TBT 협정 관점에서의 쟁점

TBT 협정 조항	주요 내용	CSP 관련 사례
제2.2	기술규정이 무역에 불필요한 제한을 주지 않아야 함	중국 정보보안 등급 보호제도(MLPS) 등 지역별 CSP 요구가 비EU·비중국 기업의 기술 진입 차단
제2.4	국제표준에 근거한 기술 규정 채택	일부 CSP는 ISO/SOC 등과 별개로 자체 기술 심사 적용
제2.5	기술규정 제정 시 목적·근거·과학성 제공 의무	CSP가 자의적으로 정보를 요구하거나 심사 기준을 비공개
제5.1	적합성 평가 절차는 공정하고 투명해야 함	CSP의 판매자 검토(vendor review), 기초기술검토(FTR) 등 심사 프로세스 불투명성 문제

산업계 대응방안

CSP 입점 심사에 대비해 서비스형 소프트웨어(SaaS) 기업이 자체적으로 점검해야 할 기술 및 법률 요건을 사전에 파악하고, 기업은 기술 설계뿐 아니라 문서화, 인증, 법률 대응 체계를 사전에 구축해야 함

- CSP 요건은 국제표준에 근거하되, 자체 기준으로 해석 및 심사 진행
- 특히 중소 SaaS 기업은 정부의 인증지원, 문서 작성 지원, TBT 분석 가이드 등을 활용해 입점에 따른 위험부담을 낮출 수 있도록 대응방안 수립이 필요함

[표 14] CSP 입점 대응 체크리스트*

구분	항목	점검여부
보안설계	□ IAM 역할/정책 분리 구성 되어 있는가?	☐
보안설계	□ 저장 데이터는 AES-256, 전송은 TLS 1.2 이상 적용되었는가?	☐
보안운영	□ 취약점 점검 및 패치 대응 프로세스 존재 여부	☐
법적문서	□ 개인정보처리방침(영문) 공개 및 최신화 상태	☐
법적문서	□ GDPR 대상일 경우 DPA 및 SCC 준비 여부	☐
개인정보	□ 개인정보 동의/철회/열람/삭제 기능 구현 여부	☐
인증자료	□ SOC 2 또는 ISO/IEC 27001 인증 보유 여부	☐
문서화	□ CSP 심사용 보안/프라이버시 설계 문서 준비 여부	☐
리전정책	□ EU/중국/러시아 등 지역별 데이터 저장 요구 대응 여부	☐
고객지원	□ SLA, 지원정책, 약관 등 Marketplace 등록 문서 구비 여부	☐
※ 점검 결과 중 7개 이상 “X”일 경우, 입점 준비 부족 가능성 높음		

* 해당 체크리스트는 Microsoft Azure Marketplace에 SaaS 또는 관리형 애플리케이션을 신속하게 등록 및 판매할 수 있도록 지원하는 플랫폼 ‘WeTransact’의 ‘Azure SaaS 목록 규정 준수 체크리스트’를 참조함

4 관련 법령

관련 법령

국가	법령 텍스트
EU GDPR	General Data Protection Regulation 공식 텍스트 및 해설 (eur-lex.europa.eu)
미국 CCPA	캘리포니아 소비자 개인정보 보호법 (ccpa.ca.gov)
싱가포르 PDPA	Personal Data Protection Act (pdpc.gov.sg)
중국 사이버 보안법	중국 공식 영문법령 + DigiChina 번역 해설 (https://digichina.stanford.edu/)

5 참고 자료

참고 자료

기관	제목 (링크)
유럽 집행위원회	▪ 유럽 집행위원회(European Commission) 공식 사이트 https://ec.europa.eu/info/index_en ▪ Shaping Europe's digital future https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en
EU 법령 포털	▪ EU 법령 포털 http://eur-lex.europa.eu
ISO	▪ ISO Standards https://www.iso.org/standard ▪ ISO/IEC JTC 1/SC 42 인공지능 https://www.iso.org/committee/6794475.html
미국 국립표준국	▪ AI Risk Management Framework https://www.nist.gov/itl/ai-risk-management-framework
OECD	▪ Artificial intelligence https://www.oecd.org/en/topics/artificial-intelligence.html
일본 경제산업성	▪ 일본 경제산업성 공식 사이트 https://www.meti.go.jp
캐나다 과학, 경제 개발부	▪ Artificial Intelligence and Data Act https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act
영국 과학 및 혁신기술부	▪ 영국 과학 및 혁신기술부 https://www.gov.uk
AWS	▪ What is AWS Marketplace? https://docs.aws.amazon.com/marketplace/latest/userguide/what-is-marketplace.html ▪ AWS Marketplace Vendor Insights 이해 https://docs.aws.amazon.com/ko_kr/marketplace/latest/userguide/vendor-insights-understanding.html ▪ Updates to the AWS Foundational Technical Review https://aws.amazon.com/ko/blogs/apn/aws-foundational-technical-review-expands-to-include-serivice-offerings/ ▪ Vender Insigjts https://aws.amazon.com/marketplace/features/vendor-insights/

Suger	▪ A Guide to 9 Common AWS Marketplace Listing Mistakes (And How to Avoid Them) https://www.suger.io/blog/common-aws-marketplace-listing-mistakes
Microsoft Ignite	▪ Microsoft Publisher Agreement 8.0 July 2024 update https://learn.microsoft.com/en-us/legal/marketplace/msft-publisher-agreement
WeTransact	▪ Azure SaaS Listing Compliance Checklist https://www.wetransact.io/blog/azure-saas-listing-compliance-checklist?
Google Cloud	▪ Sensitive Data Protection release notes https://cloud.google.com/sensitive-data-protection/docs/release-notes ▪ Google Cloud Trust Center https://cloud.google.com/trust-center
한국표준협회	▪ 인증 및 검증 https://ksa.or.kr/ksa_kr/7011/subview.do
AICPA & CIMA	▪ Standards and Statements https://www.aicpa-cima.com/resources/landing/standards-and-statements
세계법제정보센터	▪ 싱가포르 개인정보보호법(Personal Data Protection Act 2012) https://world.moleg.go.kr/web/wli/lgslInfoReadPage.do?CTS_SEQ=41904&AST_SEQ=277

심층분석보고서

관련 심층분석보고서

– 동 규제와 관련된 심층분석보고서는 KnowTBT 포털(knowtbt.kr)에서 열람 가능 (URL 바로가기)

* 열람 경로: KnowTBT 포털(Knowtbt.kr) 접속 → 규제정보 → 시행예고 규제 → WTO 미통보 정보 → 규제정보 검색

특정무역현안(STC)

특정무역현안(STC) 제기 여부

– 중국 사이버 보안법과 관련하여, 현재까지 WTO TBT 위원회에서 특정무역현안(STC)*으로 제기되어 WTO 회원국 간에 논의된 이력은 다음과 같음**

* **특정무역현안(Specific Trade Concern, STC)**이란, WTO 회원국이 다른 회원국의 기술규제, 표준, 적합성평가 절차 등이 자국의 무역에 부정적인 영향을 미치거나 미칠 우려가 있다고 판단하여 WTO TBT 위원회 등의 공식 회의에서 제기하는 사안을 의미함

** 하기 [표 17] 외에 추가 STC 이력 및 발언문 원문(영문)은 다음 URL에서 확인 가능 (STC 확인하기)

[표 17] 2025년 제1차 WTO TBT 위원회 STC 내용

국가	제기 내용
미국	- 중국의 보안 테스트 및 ICT 구매 기준은 복잡하며 미국 기업에 중대한 부담 - 과거 회의에서 제기한 문제들이 여전히 해결되지 않음
일본	- '핵심 데이터'의 모호한 정의가 사업 예측 가능성 저해 - 위험평가·보고 의무의 기준이 추상적이며 기업에 과도한 부담 초래 - 국경 간 데이터 흐름 제한이 무역에 불필요한 제약을 초래하지 않도록 요청
유럽연합	- 법률 간 정의 불확실성으로 기업에 적용 법률이 불명확 - 중요정보 인프라(CII)와 다단계 보호 체계(MLPS)의 의무 중복 지적 - 사이버보안 검토 기준이 광범위하고 불투명함 - 제품/서비스 카탈로그 등 투명하게 통보되지 않음 - 투명성·비례성·기술 중립성 준수 요청
호주 (지지)	- 초영토주의, 무역 보복, 준수 비용 증가 등 우려 - 관련 법률 시행 시 기업 의견을 고려해줄 것 요청
캐나다 (지지)	- 지역별 상이한 국경 간 데이터 전송 요건이 혼란 초래 - 다수의 조치가 통보 없이 진행됨 - 특히 중소기업에 시장 접근 제한, 경쟁력 저하 발생 - 사이버보안·데이터보안 법령이 WTO TBT 원칙에 부합하지 않을 수 있음
중국 답변	- 사이버 보안법은 국가 안보·공공 이익·사이버 주권을 위한 기본법 - 법 시행 이후 관련 규정이 점진적으로 개선 중 - 디지털 경제의 안전한 발전에 기여하고 있다고 주장

주 의

ㅇ 본 보고서는 산업통상자원부 국가기술표준원의 무역기술장벽(Technical Barriers to Trade, TBT) 대응 활동의 일환으로 최신 규제 정보를 제공하기 위해 작성되었습니다.

ㅇ 본 보고서는 TBT종합지원센터의 동의 없이 무단 배포 및 변경할 수 없으며, 상업·법률적 판단 근거로 활용될 수 없습니다.

ㅇ TBT종합지원센터에서 운영 중인 KnowTBT 포털을 통해 더 많은 해외 기술규제 정보를 제공 받을 수 있습니다 (www.knowtbt.kr).

Tel. : 02-3487-7758 **Fax** : 02-571-0003 **E-mail** : tbt@kotica.or.kr