Deloitte.

급변하는 데이터 규제 환경 속 소버린 클라우드 전략 부상

Ben Stanton 딜로이트 TMT Insights Manager 외 5인

2024년 3월
Deloitte Insights

데이터 증가, 사이버위협 고도화, 지정학적 긴장 고조 등으로 클라우드 솔루션의 현지화에 대한 수요가 늘고 있다. 클라우드 기업들은 이러한 니즈를 충족해야 평판과 매출을 사수하고 운영 회복력을 강화할 수 있다.

2024년 전 세계에서 149제타바이트(zettabyte)의 데이터가 생성될 것으로 전망된다.[1] 제타바이트는 '기가바이트(gigabyte)×1,000×1,000×1,000×1,000...'에 해당하는 데이터 단위다. 1바이트가 모래알 하나라면, 1제타바이트는 전 세계 해변을 2만 번 정도는 가득 채울 수 있는 규모다.[2] 이 정도 규모의 데이터 생성과 프로세싱이 가능한 것은 클라우드 덕분이다.

클라우드는 2023년 시장 규모가 6,000억 달러에 육박해[3] 범산업적 펀더멘털이자 주요 산업으로 자리잡았다. 디지털 전환의 엔진 역할을 하면서 서비스의 품질을 개선하고 시간을 단축했을뿐 아니라, 인력 기동성을 강화하고, 애널리틱스와 인공지능(AI)의 새로운 지평을 열었다. 클라우드 컴퓨팅은 위치와 무관하게 데이터를 생성 및 처리할 수 있다는 개념에 기반한다. 규모의 경제나 컴퓨팅 자원을 극적으로 확대하지 않아도 데이터 인프라를 활용할 수 있는 것이다. 클라우드의 이러한 혁신에 힘입어 데이터의 양과 가치와 함께 민감도가 심화되며, '소버린 클라우드'(sovereign cloud) 개념이 등장했다. 즉 클라우드에 저장된 데이터는 그 데이터가 물리적으로 위치한 국가의 법을 적용받는다는 원칙이다. 소버린 클라우드는 점차 정책입안자들이 지대한 관심을 쏟는 사안이 됐다.

2024년 모든 선진국에서 클라우드 주권에 대한 정책입안자들의 논의가 한층 높은 차원으로 심화될 것으로 전망된다. 이와 함께 각 정부의 엄격한 컴플라이언스 규정에 부합하기 위해 설계된 솔루션인 공공 클라우드(government cloud) 시장 규모가 2024년 410억 달러를 넘어, 전년 대비 16% 성장할 것으로 예상된다.[4] 또한 데이터가 실제 보관되는 지리적 위치를 뜻하는 데이터 레지던시(data residency) 제한에 대한 솔루션으로 등장한 분산 클라우드(distributed cloud) 시장은 2022년 약 40억 달러에서 2024년에는 70억 달러에 달할 것으로 전망된다.[5]

클라우드 컴퓨팅의 시초

클라우드 컴퓨팅 개념을 이해하려면 인터넷 초창기 시절로 거슬러 올라가야 한다. 1960년대 시분할(time-sharing) 시스템에서 시작해,[6] 1990년대 가상 사설 통신망(virtual private network, VPN)을 거쳐,[7] 2000년대 중반 아마존웹서비스(AWS)가 등장해 패러다임이 완전히 변했다.[8] AWS는 규모 확대가 가능한 온디맨드(on-demand) 컴퓨팅을 불특정 다수의 대중에게 제공했다. 곧 구글(Google)과 마이크로소프트(Microsoft) 등도 클라우드 플랫폼을 출시해, 클라우드를 현대 디지털 환경의 기본 인프라로 만들었다.

이후 지난 20년간 기업, 정부, 기관, 개인은 점차 데이터와 워크로드를 사무실의 서버랙(server rack) 등 자체 인프라로부터 단일 클라우드 데이터센터로 옮겼다. 그 과정에서 새로 등장한 클라우드 네이티브 애플리케이션도 상당수 도입됐다. 방대한 데이터가 글로벌 네트워크를 넘나들며 저장 및 이동되자, 데이터의 주권, 거버넌스, 소유권 등에 대해 우려하는 정부와 기업이 나타났고, 이에 소버린 클라우드 개념이 확산되기 시작했다.

다국적 기업의 난제...국가·지역마다 상이한 데이터 규제

데이터 현지화법은 다국적 기업들에게 언제나 운영상의 복잡성을 안겨주는 난제다. 각국 정부가 국가안보, 데이터 보호, 신기술 등과 씨름하며 규제가 바뀌는 일이 비일비재한데, 데이터와 자동화, AI에 대한 기업들의 의존도는 높아지기 때문이다. 이에 기업들은 규제가 어떻게 수정, 철회, 보강되는지 항시 예의주시해야 한다. 오늘날 운영 민첩성만큼이나 컴플라이언스가 기업 운영에 매우 중요하기 때문이다. 하지만 수백개국 정부가 저마다의 상황에 따라 각기 다른 규제를 도입하고 있어, 다국적 기업들은 국가와 지역마다 상이한 데이터 규제에 부합해야 한다는 난제를 안고 있다.

지금까지 미국과 유럽연합(EU)이 대서양 횡단 데이터 흐름에 대한 공통 규제를 마련하려 몇 차례 시도했으나, 대부분 유럽사법재판소에 의해 무산됐다(그림 1). 한편 지난 10년간 EU 일반 데이터 보호 규정(GDPR), 미국 '클라우드법'(CLOUD Act), 미국 캘리포니아주(州)의 '개인정보보호 권리법'(CPRA) 등 데이터 주권 관련 규제가 마련됐다.

이처럼 데이터 주권 규제가 산발적으로 도입되면서 글로벌 기업들의 운영 복잡성이 심화되고 있다. 예를 들어, 미국 클라우드법에 따르면 특별 법률집행 목적에 부합한다면 당국이 외국에서 저장된 데이터에 접근할 수 있으나, EU GDPR에 따르면 개인정보는 '충분한 수준'의 데이터 보호가 이뤄져야만 유럽경제지역 외부로 이동할 수 있다.[9] 클라우드법은 따랐으나 GDPR을 어겼다면 해당 기업은 막대한 벌금을 내야할 수 있다.[10] 영국과 미국처럼 양자 협정에 따라 동일한 규제가 적용될 수도 있지만,[11] 이를 위해서는 시간이 오래 걸린다. 이러한 규제의 복잡성을 우회하기 위해 기업들이 자주 사용하는 방법은 종단간 암호화(E2E encryption)다. 데이터가 발신원에서 수신원까지 전송될 때까지 암호화를 유지하는 것이다. 이렇게 되면 클라우드 기업이 해당 데이터를 집행 당국에 넘겨줘도, 해독 키 없이는 데이터를 복화할 수 없다.

그림 1. 대서양 횡단 데이터 전송에 대한 미국-EU 규제 및 협정 관련 주요 이슈

2000년	**세이프 하버 협정 (Safe Harbor Agreement)**	미국-EU 간 개인신상정보 전송에 관한 협정으로, 미국 상무성 세이프 하버에 등록하고 유럽의 개인정보보호 지침을 준수하면 개인정보를 미국으로 전송할 수 있도록 했다.[A]
2013년	**에드워드 스노든의 내부고발 (Snowden Revelations)**	미국 국가안보국(NSA)의 컴퓨터 기술자로 일했던 에드워드 스노든이 NSA의 개인정보보호 침해, 정부 사찰 등에 대한 기밀자료를 폭로하면서 데이터 주권에 대한 논의가 촉발됐다.
2015년	**세이프 하버 협정 무효화 (Schrems I)**	미국 정부 사찰 관련 법이 EU의 개인정보 보호 규정을 위반할 우려가 있다며 유럽사법재판소가 세이프 하버 협정에 무효 판결을 내렸다.[B] 오스트리아 활동가 겸 법대생이었던 막스 슈렘스(Mark Schrems)가 페이스북을 상대로 유럽사법재판소에 제기한 소송이 계기가 된 판결이라 'Schrems I'이라고도 불린다.
2016년	**EU-미국 프라이버시 실드 (EU-US Privacy Shield)**	EU와 미국이 세이프 하버 협정의 단점을 보완해 대서양 횡단 데이터 전송을 위한 새로운 프레임워크를 마련했다.[C]

2016년	**EU 일반 데이터 보호 규정 (GDPR)**	EU는 역외 데이터 전송에 대한 엄격한 규제를 마련해, EU 내 개인정보가 적절한 보호 조치 없이 역외로 전송되지 못하도록 의무화했다.[D]
2018년	**미국 클라우드법 (CLOUD Act)**	특별 법률집행 목적에 부합한다면 데이터의 지리적 위치와 상관없이 집행 당국이 테크 기업들이 보유한 개인정보를 요구할 수 있는 클라우드 법이 제정됐다.[E]
2020년	**EU-미국 개인정보보호 체계 무효화 (Schrems II)**	미국 정부 사찰 관련 법이 EU의 개인정보 보호 규정을 위반할 우려가 있다며 유럽사법재판소가 EU-미국 프라이버시 실드에 무효 판결을 내렸다.[F]
2023년	**EU-미국 데이터 프라이버시 프레임워크 (EU-US Data Privacy Framework)**	미국과 EU 지도자들이 메커니즘 수정 내용과 대서양 횡단 데이터 흐름을 감시하는 '정보 보호 검토 법원'(Data Protection Review Court, DPRC)의 신설 등 내용을 포함해 EU-미국 프라이버시 실드를 대체할 새로운 프레임워크를 발표했다.[G]

출처: A - Ernst-Oliver Wilhelm, "A brief history of Safe Harbor (2000–2016)," International Association of Privacy Professionals (IAPP), accessed November 20, 2023. / B - Court of Justice of the European Union, "The Court of Justice declares that the Commission's US Safe Harbour decision is invalid," press release, October 6, 2015. / C - European Commission (EC), "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield," press release, February 2, 2016. / D - EU, Directive 95/46/EC (General Data Protection Regulation). / E - US Congress, Clarifying Lawful Overseas Use of Data Act or the CLOUD Act. / F - Hendrik Mildebrath, "The CJEU judgment in the Schrems II case," European Parliamentary Research Service (EPRS), September 2020. / G - EC, "Adequacy decision for the EU-US Data Privacy Framework," July 10, 2023.

복잡한 규제 환경에 대응하려면 데이터 관리가 필수다. 기업들은 다양한 데이터를 규제 컴플라이언스에 맞춰 개인정보, 결제 데이터, 재무 규제 정보 등으로 분류할 필요가 있다. 또한 데이터 주권 침해나 규제 변화 소지가 있다면 클라우드 업체를 바꿀 수 있도록 '출구 전략'도 미리 마련해야 한다. 하지만 클라우드 서비스 계약이 통상 5년 이상 단위로 이뤄지고 클라우드간 데이터를 이동하는 데에도 막대한 비용이 소요되기 때문에, 현실적으로 클라우드 벤더를 바꾸는 것은 쉽지 않다.

글로벌 사안으로 부상한 데이터 주권

미국과 EU뿐 아니라 세계 각국에서 데이터 주권 프레임워크를 마련하려는 움직임이 일고 있다. 미국과 EU 외 대표적 사례는 다음과 같다.

- ☑ 러시아는 데이터 주권과 관련해 세계에서 가장 먼저 가장 엄격한 규제를 마련한 국가 중 하나다. 러시아 연방법 No.242-FX에 따르면, 러시아 시민의 개인정보는 러시아 국경을 넘을 수 없다.[12] 이에 따라 2016년 이후 러시아에서는 링크트인(LinkedIn) 접속이 제한되는 등 글로벌 기업과 브랜드가 러시아에서의 활동에 큰 제약을 받고 있다.[13]

- ☑ 2017년 제정된 중국 '사이버보안법'에 따르면, 핵심 정보 인프라 운영자들이 중국에서 수집 및 생성한 개인정보와 중요 기업 데이터는 중국 영토 내에서 저장돼야 한다.[14] 중국 정부는 2021년 '데이터안전법'과 '개인정보 보호법'을 제정해, 데이터 분류를 의무화하고 이에 기반해 국경간 데이터 전송에 대한 규제를 강화했다.[15]

- ☑ 사우디아라비아는 2018년 '클라우드 컴퓨팅 규제 프레임워크'(CCRF)를 도입해,[16] 클라우드 서비스 제공자들에게 적용되는 데이터 주권 조건을 명시하고 특정 유형의 데이터에 대한 데이터 레지던시를 의무화했다. 이후 2021년에 '개인정보 보호법'을 제정해, 제한된 조건 하에서만 시민의 개인정보를 국외로 전송할 수 있도록 했다.[17]

데이터 주권 논의의 주요 쟁점

데이터 주권은 이미 중요한 글로벌 논의 사안이 됐으며, 갈수록 중요성이 커지고 있다. 특히 러시아-우크라이나 전쟁과 같은 지정학적 요인부터 하이브리드 및 멀티 클라우드 등장에 따른 클라우드 복잡성 등 기술적 요인, 데이터 보호와 사이버보안 등 규제 요인까지 광범위한 이슈들이 얽혀 데이터 주권 논의를 복잡하게 만들고 있다. 이 가운데 전 세계의 데이터 의존도는 빠르게 심화되고 있으며, 클라우드가 데이터 저장·관리·분석을 위한 사실상의 솔루션으로 자리잡을 가능성이 있다.

기업 vs. 정부 입장 차이

국가안보와 개인정보보호 간 균형을 맞추는 일은 종종 딜레마에 처한다. 그리고 과거 데이터 관련 세간의 이목을 끄는 사건들로 인해 각국 정부들이 적극적으로 데이터에 대한 사법적 경계를 설정하게 됐다. 대표적으로 2016년 미 연방수사국(FBI)이 샌버나디노 총기 난사 사건 용의자의 아이폰5C를 입수해 애플(Apple)사에 잠금 해제를 요청했으나, 애플은 보안 우려를 내세우며 협조를 거부한 바 있다.[18] 이 사건은 국가간 분쟁으로 볼 수는 없지만, 국가 안보기관과 개인정보보호 권리 및 테크 기업들의 사용자 데이터 보호 책임 간 충돌 지점을 단적으로 보여줬다. 2013년에는 실제로 미국의 사법 관할권 외 지역에서 정부와 기업 간 충돌이 빚어졌다. 당시 미국 법무부가 마약사범 수사를 위해 마이크로소프트(MS)에 이메일 정보 제공을 요구했으나, MS는 해당 정보가 아일랜드 서버에 저장돼 있다는 이유로 협조를 거부했다.[19]

지정학적 불안정에 따른 데이터 주권 혼란

열강들 사이 긴장이 고조되면서 첨단기술과 데이터가 외교 및 무역 분쟁의 중심 이슈가 되고 있다.[20] 러시아의 침공이 임박하자 우크라이나 정부가 인구 등록 정보, 토지 및 부동산 등기, 세금 납부 내역, 교육 기록 등 핵심 데이터를 클라우드로 재빨리 이전하면서, 데이터 주권 문제가 다시금 국제사회의 화두로 떠올랐다.[21] 한편 미국 소재 클라우드 서비스 업체들은 러시아의 침공 직후 러시아 내에서 클라우드 서비스 판매를 중단했다.[22]

클라우드 복잡성 심화

당초 클라우드를 이용한다는 것은 자체 온프레미스(on-premise) 운영 체계를 단일 클라우드 서비스로 옮기는 것이 일반적이었다. 하지만 오늘날 기업들은 동시에 여러 개의 클라우드 플랫폼을 사용해 멀티클라우드(multi-cloud) 환경이 조성됐다. 각각의 플랫폼이 제공하는 각기 다른 기능을 활용하고 비용과 기능을 최적화하고 규모를 용이하게 조절하기 위함이다. 이와 함께 온프레미스와 퍼블릭 클라우드를 함께 사용하는 하이브리드 클라우드(hybrid cloud) 사용도 확산되고 있다. 민감한 데이터를 다루는 애플리케이션은 온프레미스로 운영하고 여타 워크로드는 퍼블릭 클라우드의 방대한 자원을 활용해 처리하는 것이다. 멀티클라우드와 하이브리드 클라우드 모두 유연성과 최적화라는 장점이 있지만, 복잡성의 문제도 수반한다. 특히 데이터가 다양한 운영 환경에 퍼져 있다 보니, 데이터 관할권의 경계를 넘는 일이 종종 발생한다. 클라우드 벤더는 대부분 복수의 국가에서 데이터센터를 운영하기 때문에, 각국의 상이한 데이터 규제가 적용된다. 이에 따라 데이터 주권의 관리와 거버넌스가 여느 때보다 복잡해졌다. 한 국가의 규제만 따라서는 안 되며, 글로벌 규제 환경의 복잡한 실타래를 정확하게 파악해야 컴플라이언스 문제에 대처할 수 있다.

데이터 보호 및 사이버보안

대체로 클라우드 컴퓨팅으로 실현되는 생성형AI와 머신러닝, 자동화는 기업 운영에 필수 요인이 되고 있다. 이에 각국 정부는 데이터 주권에 대해 더욱 세부적인 규제를 적용할 수밖에 없다. 이 가운데 갈수록 늘어나는 데이터 침해를 막기 위해 데이터 현지화가 리스크를 완화하는 수단으로 간주되고 있다. 2020년 솔라윈즈(SolarWinds) 해킹 사건으로 1만8,000개 이상의 정부기관과 기업이 피해를 입은 후 중앙화 클라우드 시스템의 취약성이 부각됐다.[23] 당시 러시아 해커들이 솔라윈즈의 모니터링 솔루션인 '오리온'(Orion)에 멀웨어를 심어 통상적 소프트웨어 업데이트를 통해 악성코드를 유포시켰다. 이 사건으로 데이터 보안과 주권이 개별적 차원이 아닌 공급망 전체 차원에서 강화돼야 한다는 인식이 확산됐다. 기업들은 사용 중인 서비스형 소프트웨어(SaaS)와 벤더에 대한 철저한 조사를 통해 어떠한 클라우드 플랫폼을 사용하는지, 어떠한 데이터가 클라우드에서 처리되는지, 암호화는 어떤 수준인지, 어떠한 리스크가 수반되는지 정확하게 파악해야 한다. 또한 이러한 해킹 사건으로 각국 정부는 시민의 개인정보에 대한 통제와 감시를 강화해야 한다는 압박을 받게 됐다. 앞으로도 사이버 보안 과제는 심화될 것이다. 사이버범죄에 따른 비용은 2024년 14조6,000억 달러로 2021년의 6조 달러에서 두 배 이상 증가할 것으로 전망된다.[24]

데이터 주권은 지리적 위치에 국한되지 않고, 운영과 거버넌스의 개념으로 확대된다. 암스테르담 트레이드 뱅크(Amsterdam Trade Bank, ATB)가 대표적인 사례다. ATB는 네덜란드에 위치했지만 러시아 알파방크(Alfa-Bank)의 자회사로 러시아인이 지분 42%를 소유하고 있다는 이유로 2022년 미국 정부의 제재 대상이 됐다. ATB의 데이터는 유럽에 위치했지만, 해당 데이터를 운영한 클라우드 벤더가 미국 소재 업체였기 때문에 ATB의 이메일 계정과 관련 데이터에 대한 접근 권한을 차단할 수 있었다. 이처럼 일부 국가의 정부는 데이터가 지리적 관할권 내에 위치하는 것뿐 아니라 클라우드 인프라 운영자도 현지 업체여야 한다고 요구하고 있기 때문에, 클라우드 벤더들은 이러한 리스크에 대응하기 위해 현지 벤더와 협업하는 방식을 모색하고 있다.[26]

전 세계가 디지털로 한층 결속되면서, 경계를 세분화하고 보안을 지키며 시민의 권리를 보호하는 것이 여느 때보다 중요해졌다. 그 결과 지정학적 요인, 보안 우려, 개인의 권리 보호 등에 영향을 받는 데이터와 클라우드 주권을 둘러싼 논의는 향후 수년간 더욱 심화될 것이다.

소버린 클라우드 솔루션, 클라우드 업계에 기회이자 과제

클라우드 서비스 벤더들은 데이터 주권이 갈수록 중요한 이슈로 부각되는 것을 반영해 다양한 제품과 서비스, 사양을 출시하고 있다. 엄격한 규제 컴플라이언스에 맞춤화한 공공 클라우드가 데이터 주권을 고려한 대표적인 서비스다.

클라우드 벤더들은 고객사 입장에서 데이터 주권 리스크를 줄이기 위한 솔루션도 제공하고 있다. 클라우드 인프라 전체를 고객의 온프레미스 시스템으로 옮겨[27] 고객이 클라우드 서비스를 자체 데이터센터에서 운영해, 데이터가 온프레미스 상태 또는 특정 국가를 벗어나지 않게 하는 것이다. 이 외에도 데이터가 특정 지역을 벗어나지 않게끔 다양한 솔루션으로 구성된 포트폴리오가 제공되고 있다.[28]

이러한 솔루션은 모두 분산 클라우드라 불리기는 힘들지만 분산 클라우드와 비슷한 서비스라 볼 수 있다. 분산 클라우드는 다양한 물리적 위치에 퍼블릭 클라우드를 분산하면서도 운영, 거버넌스, 업데이트 등은 클라우드 운영 벤더의 책임으로 남게 된다. 한 마디로 데이터가 생성 및 소비되는 곳과 지리적으로 가까운 위치에 클라우드를 배치하는 것이다.

이러한 솔루션은 지연 단축 등 여러 장점이 있지만, 기존의 클라우드 서비스에서는 나타나지 않았던 문제를 수반할 수 있다.

비용	분산 클라우드 솔루션은 기존 종량제(pay-as-you-go) 클라우드 서비스와 달리 하드웨어 및 인프라에 대한 사전 투자가 필요하다. 또 소프트웨어 스택은 클라우드 벤더가 관리하지만, 온사이트 하드웨어를 관리하려면 추가 비용이 들 수 있다. 게다가 분산 클라우드 환경을 효율적으로 관리 및 운영하면 IT 팀 교육도 필요하다.
복잡성	분산 클라우드를 기존 온프레미스 시스템에 통합하는 것은 복잡한 일이 될 수 있다. 하이브리드 또는 멀티 클라우드를 활용하려면 다양한 환경에서 워크로드를 관리해야 하기 때문이다.
제한적 서비스	분산 클라우드에서는 퍼블릭 클라우드가 제공하는 기능을 모두 사용하지 못할 수 있다. 또한 중앙화 클라우드의 기능과 업데이트가 분산 클라우드에 적용되려면 추가로 시간이 걸린다.
규모 확대 어려움	기존 클라우드 서비스는 무제한 규모 확장이 가능하지만, 분산 클라우드 솔루션은 로컬 인프라의 역량에 따라 규모 확대가 제한될 수 있다. 기존 클라우드는 소프트웨어 업데이트로도 충분히 역량을 확대할 수 있지만 분산 클라우드는 하드웨어에 대한 추가 투자가 필요하다.
벤더 종속 (lock-in)	특정 클라우드 벤더의 분산 솔루션에 의존하면, 상당한 노력과 비용을 들이지 않고서는 다른 벤더로 교체하거나 멀티 클라우드 전략으로 전환하기 힘든 벤더 종속 문제가 발생할 수 있다.
성능 부족	온프레미스에 배치한 분산 클라우드 하드웨어의 성능은 클라우드 벤더의 데이터센터 인프라보다 떨어지는 경우가 있다. 온프레미스나 엣지 솔루션을 이용 중이더라도, 데이터를 중앙 클라우드로 전송해야 할 경우가 생겨 네트워크 병목현상이 발생할 수 있다.

클라우드 벤더들에게 소버린 클라우드 수요 증가는 고가치 서비스 판매를 늘릴 수 있는 기회로 작용하지만, 수익성을 갉아먹는 요인이 될 수도 있다. 벤더들에게 가장 유리한 결과는 제한 없이 모든 국가에서 하이퍼스케일 퍼블릭 클라우드를 판매하는 것이다. 하지만 국가별 상이하고도 엄격한 컴플라이언스 의무에 맞춰 아키텍처가 다양하게 설계돼 있어, 글로벌 클라우드 인프라도 산발적으로 구축돼 있다. 이로 인해 벤더들은 고가치 서비스를 더 비싼 값에 판매하더라도 운영비 증대와 마진 압박에 직면할 수 있다. 하지만 소버린 클라우드 수요와 함께 하이브리드 클라우드와 인프라 수요가 증가하면, 로컬 서비스 벤더와 기존 하드웨어 벤더들에게는 호재가 될 수 있다.

결론: 선제적으로 소버린 클라우드 전략을 수립하라

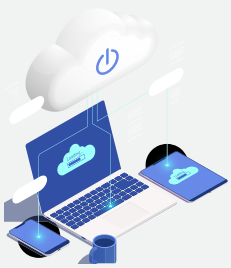
현대 글로벌 디지털 경제에서 활동하는 기업들에게 데이터 저장·관리·처리에 대한 규제를 준수하는 것은 무엇보다 중요하다. 그렇지 않으면 심각한 처벌과 벌금에 처할뿐 아니라 고객과 파트너사의 신뢰도 잃을 수 있다. 지정학적 여건과 규제 환경이 지속적으로 변화하고 개인정보보호에 대한 우려도 심화되면서, 데이터와 클라우드 주권을 지킬 수 있는 기업의 능력은 곧 시장 평판, 운영 효율성, 수익으로 직결된다. 따라서 기업들은 다음과 같은 선제적 행동으로 변화하는 환경에 적극적으로 대응해야 한다.

첫째, 총체적인 데이터 검토를 수행해, 데이터 출처를 파악하고 민감도에 따라 데이터를 분류해야 한다. 예를 들어, 개인사용자 데이터는 익명화된 분석 데이터나 메타데이터와 다른 방식으로 관리해야 한다. 둘째, 데이터 레지던시 전략을 수립해, 지연 단축 등 기술적 필요와 규제 요건에 따라 데이터의 위치를 결정하고, 로컬 데이터센터, 분산 클라우드, 클라우드 리전(region, 데이터센터 묶음) 중 어떠한 방식을 채택할지 결정해야 한다. 마지막으로, 데이터 저장과 전송 정책을 검토해, 데이터 저장 및 전송 중 암호화가 제대로 되고 있는지 확인해야 한다. 데이터를 국외로 전송해야 할 경우, 암호화를 사용하면 미승인 접근을 차단할 수 있는 추가 보안장치로 작용한다.

현지 규제를 파악하기 위한 투자도 선제적 대응에 포함될 수 있다. 현지 전문가의 도움을 받거나 IT·법무·운영 등 다양한 부서의 인력에 대한 교육을 실시해 변화하는 규제 환경을 실시간으로 파악해야 한다. 또한 데이터가 저장 및 처리되는 방식에 대해 고객 및 공급망 파트너들과 투명하고 충분히 소통해야 한다. 공급망 파트너들이 데이터를 어디에서 저장 및 처리하는지도 파악해야 한다. 마지막으로, 데이터를 클라우드나 외국 서버에서 로컬 서버로 전송해야 할 경우에 대비해 데이터 송환 전략도 수립할 필요가 있다. 가능하다면 클라우드 벤더와 계약을 맺을 때 해당 내용을 계약 조건에 포함하는 것이 바람직하다.

데이터 주권은 클라우드 전략에 내재돼야 하며, 모든 클라우드 사용자는 다음의 세 단계를 통해 지속 가능한 소버린 플랫폼을 설계할 필요가 있다.

1. 데이터 주권에 대한 방향을 설정하고 데이터 및 워크로드 분류 등 소버린 전략을 수립한 후, 개념증명(PoC)를 실시한다.
2. 소버린 전략의 아키텍처를 구성하고 데이터 통제를 실시한다.
3. 소버린 생태계를 관리하고, 상황 관찰과 리스크 모니터링 능력을 증강할 수 있는 방법을 동원하고, 자동화와 비용 최적화 방안을 모색한다.[29]



소버린 클라우드는 다국적 기업들에게 매우 중요한 전략적 사안이다. 제대로 된 전략을 수립해 충실히 이행하면 고객 신뢰를 강화하고, 법적 리스크를 줄이고, 자사의 데이터 자산을 지킬 수 있다. 이 때 규제 환경이 항시 변화한다는 점에 유의해야 한다. 데이터가 해변의 모래라면, 규제 변화는 이를 한 번에 휩쓸어버릴 수 있는 파도와도 같다. 기업들은 규제 변화를 항시 예의주시하고 컴플라이언스를 이행해야 신뢰를 유지할 수 있다.

주석

1. IDC and Statista, "Data volume creation and consumption in the future," 2020.
2. All the Trivia, "How many grains of sand are on Earth?," April 25, 2022; Per C., "Zettabyte," TechTerms.com, last updated December 15, 2012.
3. Gartner, "Gartner forecasts worldwide public cloud end-user spending to reach nearly $600 billion in 2023," press release, April 19, 2023.
4. Deloitte estimate, based on primary research, and factoring in industry research by IMARC Group, Mordor Intelligence, Straits Research, and Data Bridge market research.
5. Markets and Markets, Distributed cloud market, August 2022.
6. By the early 1960s many people can share a single computer, using terminals . . . these are the first common multi-user systems," from "Timesharing – the first online communities," Computer History Museum, accessed November 20, 2023.
7. Septimiu-Vlad Mocan, "VPN history – Everything you need to know about VPN development over the past 25 years (and a quick glimpse of the future)," TechNadu, February 4, 2020.
8. Amazon, "Amazon.com launches Web Services, developers can now incorporate Amazon.com content and features into their own web sites; extends 'welcome mat' for developers," press release, July 15, 2002.
9. US Congress, Clarifying Lawful Overseas Use of Data Act or the CLOUD Act, H.R. 4943, 115th Cong. (2017–2018); European Union (EU), Directive 95/46/EC (General Data Protection Regulation), April 27, 2016.
10. Klaus Foitzick, "U.S. CLOUD Act vs. GDPR," activeMind.legal, February 29, 2020.
11. UK.gov, "UK/USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019]," October 7, 2019.
12. Stanford, "Amending Certain Legislative Acts of the Russian Federation as to the Clarification of the Processing of Personal Data in Information and Telecommunications Networks" July 21, 2014.
13. BBC News, "LinkedIn blocked by Russian authorities," November 17, 2016.
14. Jack Wagner, "China's Cybersecurity Law: What you need to know," The Diplomat, June 1, 2017.
15. Ryan D. Junck et al., "China's new Data Security and Personal Information Protection Laws: What they mean for multinational companies," Skadden, November 3, 2021.
16. Communications, Space & Technology Commission (CST), "Cloud computing," accessed November 20, 2023.
17. Abdulaziz Al-Bosaily, Masha Ooijevaar, and Dino Wilkinson, "Saudi Arabia issues Personal Data Protection Law," Clyde & Co., September 26, 2021.
18. Tim Bradshaw, "FBI ends stand-off with Apple over iPhone," Financial Times, April 22, 2016.
19. Leo Kelion, "Microsoft battles US over warrant for drugs case emails," BBC News, September 9, 2015.
20. Jean Gil Barroca, Alfons Buxo, and Bruno Silva Batista, "Cloud sovereignty: Three imperatives for the European public sector," Deloitte Insights, 2023.
21. Tim Anderson, "'Russian missiles can't destroy the cloud': Ukraine leader describes emergency migration," The Register, November 30, 2022.

22. Ron Miller, "Amazon, Microsoft and Google have suspended cloud sales in Russia," TechCrunch+, March 10, 2022.
23. Saheed Oladimeji and Sean Michael Kerner, "SolarWinds hack explained: Everything you need to know," TechTarget, November 3, 2023.
24. Anna Fleck, "Cybercrime expected to skyrocket in coming years," Statista Technology Market Outlook; National Cyber Security Organizations; FBI; IMF.
25. Jacob Atkins, "Solvent but bankrupt: How sanctions felled Amsterdam Trade Bank," Global Trade Review, May 31, 2022.
26. For example, see Matt Small, "Hyperscaler and VMware sovereign cloud solutions indicate that local partnerships are key to the offering," Analysys Mason, September 4, 2023.
27. AWS, "AWS Outposts family," accessed November 20, 2023.
28. Google Cloud, "Anthos," accessed November 20, 2023.
29. Deloitte, Cloud sovereignty: Unleashing the potential of sovereign cloud: A gateway to resilience and adaptability, 2023.

딜로이트 첨단기술, 미디어 및 통신 산업 전문 리더

딜로이트 첨단기술, 미디어 및 통신 산업 전문팀은 빠르게 발전하는 산업 환경 속에서 고객들의 전략적 과제들을 해결할 수 있는 최상의 서비스 경험을 제공합니다. 딜로이트 첨단기술, 미디어 및 통신 산업 전문팀은 국내외 기업의 전략수립, 회계감사, 재무자문, IT 시스템 구축 등 다양한 서비스 경험을 보유한 우수 전문인력으로 구성되어 있습니다.

Contact

김우성 파트너
Technology Strategy & Transformation리더 | 딜로이트컨설팅
Tel: 02 6099 4670
Email: wooskim@deloitte.com

안상혁 파트너
디지털부문 리더/금융산업 총괄리더 I 딜로이트 컨설팅
Tel: 02 6676 3625
Email: sanghyan@deloitte.com

박지숙 파트너
금융 IT, 오퍼레이션 리더 I 딜로이트 컨설팅
Tel: 02 6676 3722
Email: jisukpark@deloitte.com

장지영 파트너
Tech Strategy 부문 파트너 I 딜로이트 컨설팅
Tel: 02 6676 3956
Email: jiyojang@deloitte.com

강기식 파트너
Lead Architect I 딜로이트 컨설팅
Tel: 02 6676 2039
Email: gikang@deloitte.com

주형열 파트너
반도체 CoE 리더 | 딜로이트컨설팅
Tel: 02 6676 3750
Email: hjoo@deloitte.com

최호계 파트너
Technology Sector 리더 | 감사본부
Tel: 02 6676 3227
Email: hogchoi@deloitte.com

박형곤 파트너
TME Sector 리더 | 딜로이트컨설팅
Tel: 02 6676 3684
Email: hypark@deloitte.com

조명수 파트너
Digital Finance & Operation 리더
Tel: 02 6676 2954
Email: mjo@deloitte.com

박권덕 파트너
TME Sector 리더 | 딜로이트 컨설팅
Tel: 02 6676 3567
Email: gwapark@deloitte.com

앱스토어, 구글플레이/카카오톡에서 '딜로이트 인사이트'를 검색해보세요.
더욱 다양한 소식을 만나보실 수 있습니다.

Deloitte. Insights

성장전략본부 리더
손재호 Partner
jaehoson@deloitte.com

딜로이트 인사이트 리더
정동섭 Partner
dongjeong@deloitte.com

연구원
김선미 Manager
seonmikim@deloitte.com

디자이너
박주리 Consultant
jooripark@deloitte.com

Contact us
krinsightsend@deloitte.com