



# DATA SOVEREIGNTY REPORT

2013 JUN

---

## 들어가기

클라우드에는 눈에 보이지 않는 곳에서 무한한 IT 자원을 제공하는 신비한 힘을 가진 대상인 동시에, 이것 역시 지구 어디에선가 위치한 물리적 서버에 의해 돌아가는 컴퓨팅 환경이다. 하지만 회사의 데이터가 회사도 알지 못하는 지구 반대편의 서버 어딘가에 저장되면서 부터, 게임의 법칙이 바뀌고 있다. 전문가들의 소견을 빌어 IT 커뮤니티의 데이터 주권(Data Sovereignty)를 둘러싼 지식과 우려의 수위를 분석하여 보았다.

---

## Data Sovereignty 서베이

미국 오바마 대통령이 Patriot Act 의 시한연장에 서명했을 때 재미있는 현상이 일어났다. 사람들이 사는 곳에 관계없이 미국이 자신들의 데이터에 접근권한을 가질 수 있다는 우려를 하기 시작했다. 예를 들면 EU 에서 일을 하더라도 MS Office 365 는 미국회사의 제품이므로 자신의 데이터를 미국이 접근할 수 있으며 굳이 그 사실을 사용자에게 알릴 필요도 없는 것이다. 비록 EU 법안은 이런 행위를 막으려 함에도 불구하고, 이러한 규칙은 Google, Amazon 등이 이미 지키고 있다. 모두 미국 회사이기 때문.

이런 모든 사항들이 중요해지면, 다음 두 가지의 의문이 생긴다. 미국이 보여주고 있는 빅 브라더식 접근법과 Data Sovereignty 문제가 그것이다. Patriot Act 가 Data sovereignty 문제를 일으킨 주범이지만, 단지 이것은 빙산의 일각이다.

여기에 해당되는 법률 용어는 “국경간 데이터 흐름(Trans-border data flow)”인데, 모든 국가는 자국의 데이터 보호법을 갖고 있으며, 프라이버시나 보안 등의 이슈와 그 집행력에 따라 매우 다양하다. 만약 데이터가 확실하게 아는 곳에 저장되고 사용자가 룰에 친숙하게 될 때는 문제가 없다. 그러나 클라우드가 기존 전통방식을 바꾸고 있다. IDC 에서는 2013 년 까지 전 세계 IT 비용은 2 조 1 천억 불을 초과할 것으로 보고 있다. 클라우드는 그 비용 중 대부분을 차지할 것이다. 퍼블릭 클라우드 시장은 더욱 성장이 예상되며 Gartner 는 미국 내 기업 60%가 향후 그들의 퍼블릭 클라우드 비중을 늘릴 것이라고 보고한다.

그러나, 이러한 클라우드 서비스에 대한 확고한 이해는 얼마나 이루어져 있는가? 그들이 사용하는 클라우드가 호스팅되며 호스팅되는 나라에서 실질적으로 누가 접근가능한지를 알고 있을까? 이런 의문을 바탕으로 우리는 42 개국의 217 개 회사를 대상으로 Data Sovereignty 에 관한 설문을 실시하였다.

## 요약

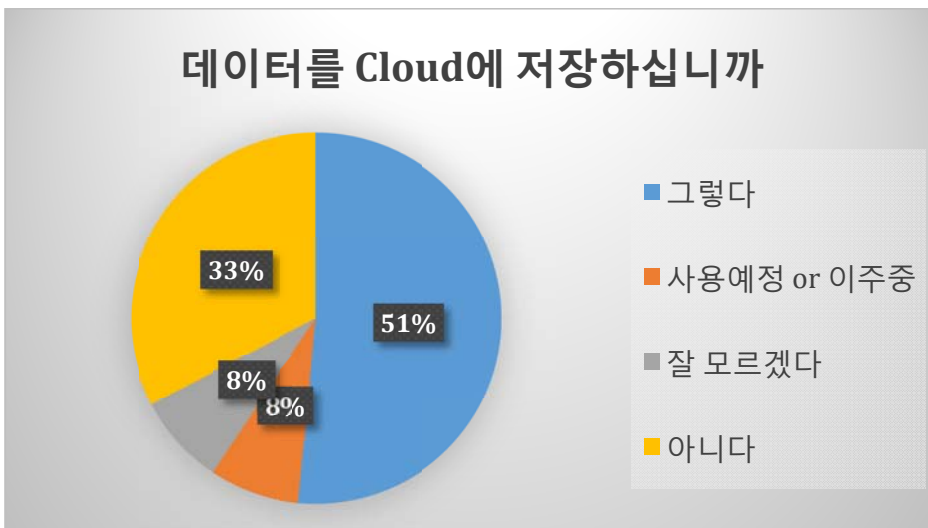
대상기업의 70%가 Data Sovereignty 에 대해 우려하고 있다

그러나 그 중 관련 법안을 정확히 알고 있는 기업은 36%에 불과하다.

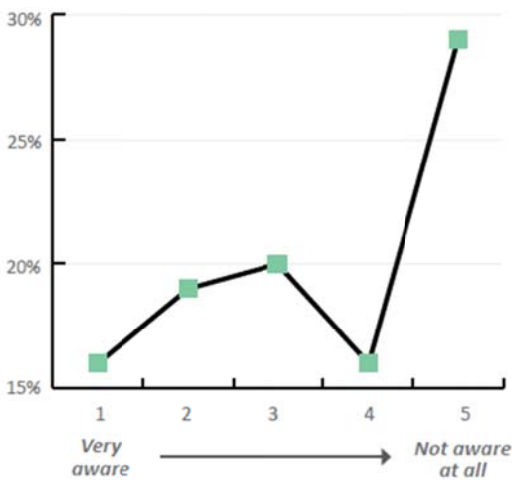
클라우드를 사용하는 기업 중, 23%만이 자신의 클라우드가 어느 나라에 있는지를 알고 있었고, 관련 데이터 법안을 알고 있었다.

현재 클라우드로 전환중인 기업 중 자신들의 클라우드가 어디에 소재하는지 아는 기업은 50%, 그러나 그들 모두 자국의 데이터 법안은 알고 있다.

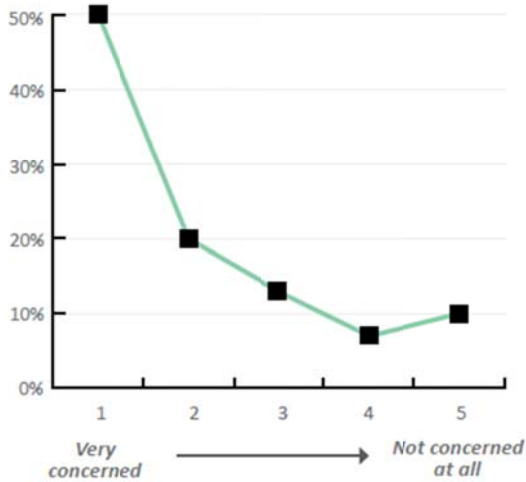
Cloud 에 데이터를 저장하는지에 대한 답변의 분포도



관련 법안을 얼마나 알고 있습니까



### Data Sovereignty 에 대해 얼마나 우려되십니까



본 서베이의 중요한 결과는, 대부분의 기업이 Data Sovereignty 에 대해 우려하고 있으나, 정작 문제에 대한 구체적인 지식은 별로 없다는 점이다. 설문대상기업의 70%는 문제에 대해 염려를 하고 있으나, 관련 법안에 대해 알고 있는 대상자는 3 분의 1 에 불과하였다. 클라우드의 사용빈도가 높고 지식이 많으면 문제를 확실히 알 것처럼 보이지만, 사실 모든 이들이 그렇지 못하고 우려만 하고 있다. 이러한 우려에는 지역을 가리지 않고 모든 지역이 이러한 우려를 갖고 있다. 기업의 60%는 서베이에서 곧 클라우드를 사용할 계획이 있거나 현재 사용 중이라고 답했는데 그 중 실제 클라우드 데이터의 소재지와 관계 법안은 불과 4 분의 1 만이 알고 있었다.

클라우드 데이터 소재지를 알고 있는 기업은 모두 Data Sovereignty 법안에 대해 이해하고 있었다. 자국의 데이터 법에 대해 잘 알고 있는 것과 별개로, 그들의 클라우드 소재지에 대해 상당히 고도의 우려를 갖고 있었다.

곧 클라우드로 이주할 계획이 있는 기업은 그 중 50%가 데이터 소재지를 알고 있었다. (이미 쓰고 있는 기업은 3 분의 1) 이주계획이 있는 기업은 거의 100%가 관련 데이터 법령을 알고 있고, 이미 쓰고 있는 기업은 절반이 알고 있었다. 그러나 현재 이주중인 기업은 데이터의 저장장소가 어디인지를 모르고 있었으며 Data Sovereignty 관련 법안에 대한 이해도도 부족했으며 전체적으로 우려를 하고 있지 않는 것으로 나왔다.

클라우드 사용중인 기업 중 63% 이 자신의 데이터 소재지를 알고 있지 못했고, 관련법안 이해도 역시 부족했다. 그러면서도 우려 정도는 높다.

#### Non-Cloud Users

설문대상자의 약 3 분의 1 은 아직 클라우드 사용계획이 없다고 했고, 이들의 법안에 대한 이해도는 다양하게 나타났으며 우려의 정도 역시 낮았다. 그러나 사실을 알면 알수록, 많이 걱정하게 된다.

Unsuers

대상자의 8%는 잘 모르겠다고 답했는데, - 당연히 Data Sovereignty 법안이해도 낮았다. 그러나 그 들 중 절반 정도는 우려를 갖고 있었다.

## 배경

오바마 미 대통령이 Patriot Act 연장에 서명하고, MS 와 같은 다국적 클라우드 기업들이 클라우드 데이터의 안전에 대해 확실한 답변을 망설이고 있는 마당에, 이제 클라우드는 더 이상 마법상자는 아니다. 클라우드 역시 어디엔가의 물리적 서버에 저장된다는 사실은 정곡을 찌르는 말일 것이다.

만일 데이터가 자국의 관할권 밖에 존재한다면 과연 어느 나라의 법을 따라야 하는가? 그 때문에 클라우드의 근거하는 기본적 위치가 최근에 갑자기 중요하여졌다.e

Patriot Act 는 그 출발점일지 모르지만, Data Sovereignty 는 훨씬 더 복잡하고 방대한 규칙체계이다.

Pirate Bay's journeyman 식 접근 방법에 의하면 데이터에 관해서 법망이 얼마나 허술한지 드러난다. 기업이 요즘에는 스위스에서 그린란드 도메인으로 옮기기가 쉽지 않지만, 이제는 서버폐쇄를 피하기 위해 클라우드로 얼마든지 피신(?) 할 수 있다. 사실 클라우드 이전에도, 정상적인 사법권이 닿지 않는 Sealand, 북한, 여러 마이크로네이션 등에 은밀한 커넥션을 갖고 있었지만.

최근 영국의 카메론 수상은 인도 국내 정부 데이터를 호스팅하기로 결정한 후 인도정부와 사이버보안 조약을 체결했다. 무모한 계획이라고 우려하는 사람들에 다시 한번 확신을 주기 위해서였다. BMW 의 IT 전문가 Lan Lamont 가 말한 대로, 브로셔에 나오는 주식 그래프쯤이야 어디에 저장되건 상관없다. 하지만 중요한 정보를 거기에 저장하라고? 말도 안 된다. 더욱 애매하게 하는 것은 데이터가 저장되는 위치에 대한 정보 부족이다. “은행 데이터가 “유럽 클라우드 리전”에 저장된다고 말하는 것은 전혀 도움이 안 된다. 유럽 클라우드 리전이 대체 어디란 말인가?

사람들은 자신의 페이스북에 올린 그림이나 무의미한 트윗을 들여다 보는 것은 개의치 않지만, 은행 계좌정보나 사적인 메시지를 누군가 입수하는 것에 대해서는 매우 예민할 것이다. 마찬가지로, 정부가 클라우드에 점차 관심을 보이고 있는 시점에서, 위험은 점차 커진다. 다른 나라에서 나의 개인적 정보를 모두 볼 수 있다는 것은 무서운 일이 아닐 수 없다. 법적으로 안전한 법망이 마련되어 있다면 괜찮다고 할 수 있다. 그러나 그것은 하나의 의견일 뿐 이다. 미디어수집수단(media grabber)으로서긴 하지만, Patriot Act 이외에도 이러한 법안이 한 두 가지가 아니고 수많은 나라들이 클라우드 데이터를 접한다는 사실은 주목할 만하다.

## 모르는 것이 약?

클라우드가 마케팅 측면에서 과장광고 된 점에도 불구하고, 아직 클라우드가 모두에게 알려진 것은 아니다. Citrix 사에 의하면, 아직도, 많은 수의 사람들(22%)가 클라우드가 기상학용어라고 생각한다. 하물며 Data Sovereignty 는 어떠한 백서는 나와 있지만, 인식은 턱없이 부족하다.

현재 당신의 데이터를 보호하면서도 클라우드의 혜택을 누리고 싶다면, 할 수 있는 선택은 별로 없다.

데이터는 인하우스에 보관하라. 당신의 데이터가 어디로 전송되는지에 신경을 쓰고, 혹 다른 곳에 저장될 때는 그에 대한 모든 사항에 대해 알고 있으라. 클라우드 제공자들은 비록 데이터 위치에 대해 공개적이긴 하지만, 데이터의 완벽한 보호를 위한 대책을 내놓는 것이 기본사항이다.

EU 통합 법안과 같이, 특정 지역을 관할하는 새로운 규칙 제정이 불가능한 것은 아니다. 그러나 그것은 어디까지나 한계가 있는 솔루션이다. 클라우드 컴퓨팅은 좀 더 다국적 개념이고, 전 세계가 따를 수 있는 통합된 룰을 가지고 있어야 할 것이다. 미국의 주마다 지역마다 상이한 규칙을 따른다면, 내 정보를 누가 보고 있는지, 염탐은 하지 않을지 등 피해망상증은 그치지 않을 것이다.

---

### 전문가 의견: George Gardiner, Gardiner & Co.

(ICT 섹터 전문 변호사)

“많은 조직들이 클라우드 Data Sovereignty 에 대한 자유방임주의적 태도의 영향을 받아 빠르고 유연하게 움직이고 있다. 재해복구와 비즈니스 연속성 이슈는 클라우드에 백업을 하면 되므로 더 이상 데이터보관사의 이슈가 아니다. 문제는 만일 클라우드 회사가 파산하거나 서비스 장애가 나면 어떻게 데이터를 보장하는가이다. 이 잘 알려진 연속성 문제를 해결하지 못하면 정말 심각한 문제이다.”

법적 조건을 맞추기 위해, 구매자들이 클라우드 서비스 제공자들과 협상할 때 데이터가 EU 영역외부에 저장되지 않도록 요구하는 경우가 점차 증가하고 있다. 주주들의 공노를 사지 않고 자신의 명성에 흠집이 나는 것을 의식해서이기도 하다. 이것은 분명 유리한 방법이지만, 최적의 관리 방식은 아니다.

“데이터의 물리적 위치는 중요한 이슈이며 EU 내에 존재한다면 그것은 문제가 되지 않는 평범한 체크사항에 불과하다. 그러나, 그렇다고 해서 클라우드 제공자가 UE Directive 의 8 원칙을 준수한다는 (특히 보안 측면에서) 것은 아니다. 제공자가 자체적인 법적 준수에 대한 약속서를 내는 것은 무의미하며, 제 3 자의 인증이 필요할 것이다. (데이터의 성격, 잠재적인 가치나 분실 시 예상되는 impact 를 고려하는)

이 시점에서 국제 인증 데이터 보안이 거론된다. 그러나, 데이터가 반드시 EU 외부로 나가지 않는다는 보장은 없다. “만일, 예를 들어, 미국 정부에서 대형 미국 회사보고 미국영토 외부 예를 들면 더블린 데이터센터의 데이터 접근을 허락하라고 한다면, 그 회사가 과연 정부의 지시를 무시할 것인가?”

언제나 위험은 도사리고 있다. 데이터센터를 완벽히 통제하지 못하는 한, 로드 밸런싱과 같은 자동화 루틴이 외부 데이터센터로 데이터를 보내지 못하란 법이 없다. 또한 Gardiner 는 중요도가 낮거나 예민하지 않은 데이터는 예외로 하자는 식의 논의는 거부한다.

“데이터 보호법은 데이터의 인지된 상업적 가치는 무시한다. 데이터는 보호가 필요한 상업적 가치를 가져야만 한다. 그렇지 않으면 왜 회사들이 비싼 돈을 들여 클라우드를 쓰겠는가?” 그는 말한다.

클라우드 구매자들은 또한 적은 상면에 익숙해져야 한다. 예를 들면 플랫폼에서는 데이터가 암호화되지만 네트워크 상에서는 암호화되지 않아, 중간에서 차단될 수 있다. 암호화되는 경우 암호화 키 소유자는 믿을 만 한가? 구두상의 심지어는 서면상의 확약이 도움이 되는 것 같아도, 회사는 처음부터 확실한 차원의 보안대책을 수립해야 할 것이다. 법안을 꼼꼼히 준수하고 있다 하더라도, 대량의 데이터 누출이 있다면 그것을 막을 도리는 없다.

지난 몇 년간 회사들은 이러한 불편한 진실에 눈뜨게 되었다. Gardiner 는 말한다. “국제 커미셔너가 글로벌 매출액의 5%까지 벌금을 물릴 수 있다는 것은 구매자들이 이러한 위험을 반드시 인지해야 한다는 것을 뜻한다.”

“클라우드를 사용하는 기업 중 중견 기업들은 이러한 사실을 모르거나, 대처할 능력조차 없다.” Gardiner 는 경고한다. “순진한 말인진 모르겠지만, 법으로는 막을 수 없다. 기술자들이 뭔가 쉬운 것을 하고자 하지만, 그런 것들이 엄청나게 심각한 법적인 잠재 위험이 있다고 알려줘야 할 때가 너무 많다. 가능하다고 해서 그것이 좋은 생각인 것은 아니다.”

## 국가별 비교: 정부의 클라우드 데이터 접근 권한

범례)

질문 1: 정부가 정부 조사의 목적으로 클라우드 제공자에게 고객정보를 요구할 수 있는가?

질문 2: 클라우드 제공자가 자발적으로 비공식적 요청에 대하여 고객정보를 정부에 줄 수 있는가?

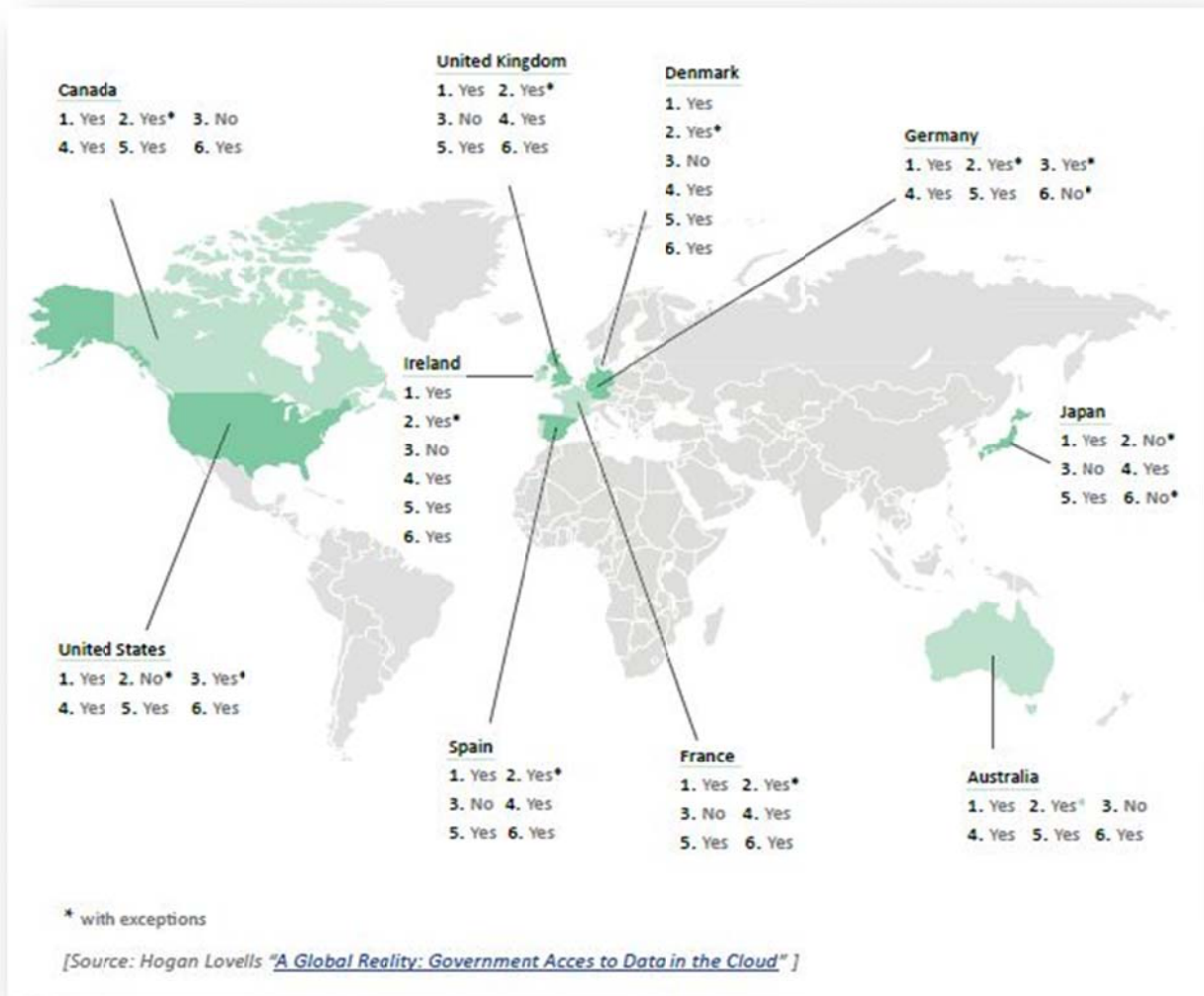
질문 3: 클라우드 제공자가 정부에 고객정보를 반드시 내야 한다면, 고객에게 이를 알려야 하는가?

질문 4: 정부가 클라우드 제공자 시스템을 통한 전자적 통신을 모니터링할 수 있는가?

질문 5: 고객정보를 제시하라는 정부의 요청은 판사의 판단대상인가?

질문 6: 클라우드 제공자가 외국 서버에 데이터를 저장시, 정부에서 그 데이터를 접근하여 요구할 수 있는가?





## 결언

Data Sovereignty 에 관한 우려는 매우 높으며, 실제 인식수준이나 지식은 부족하다는 결론이 나왔다. 데이터 위치와 안전성에 대하여 모두 잘 알고 있는 기업은 별로 없다. 이제 클라우드를 사용할 사람들은 데이터 저장위치가 어디가 될 것이며, 관련한 현지 법령에 대해 더욱 신경 써서 알아두어야 할 것이다.

비록 그럼에도 불구하고, 광의의 Data sovereignty 문제는 아직 남아 있을 것이다.