情 報 保 護 學 會 誌
第22卷 第6號, 2012. 10

EU Data Protection 개정안 이슈 및 시사점

김 상 우*

요 약

최근 mobile device, cloud computing 및 social networking 등 새로운 기술 trend의 등장으로 기존 법률 체계의 현실성 및 적절성에 대한 재검토 요구가 등장하고, 이에 따라 EU Data Protection Directive에 대한 개정안(reform proposal)이 2012년 1월 제시되었다. 따라서 새롭게 제시된 개정안의 주요 내용과 이슈, 그리고 이로부터 파생되는 시사점에 대해 고찰하고자 한다.

Ⅰ. EU Data Protection 개정안의 의미

1995년 제정된 EU의 Data Protection Directive(이하 DPD)는 개인정보보호 법률에 있어 역사적인 자취를 이뤘다고 평가되는 법률이다. DPD의 기본적인 두 가지 원칙, 즉, EU 내부 시장기능의 유지 및 개인 기본권의 효과적인 보호는 제정 이후 17년이 지난 오늘날 까지도 유효성을 인정받고 있다. 다만, EU회원국 별로 상이한 내부 법률 제정으로 인한 차이점이 개인이 어떤 EU회원국에서 상품을 구매하고 서비스를 제공받는지에 따라 상이한 법 적용을 받는 이슈를 만들어 내고 있었다. 또한, 현재의 DPD는 인터넷이 태동기인 무렵에 도입되었기에 현 상황에 맞는 현대화가 당연히 요구되고 있다. Social networking, cloud computing, 위치기반 서비스와 스마트카드 등의 최신의 기술변화와 세계화는 개인정보보호 관련 법률에 새로운 과제를 요구하고, 이러한 흐름 속에서 DPD의 개정안은 미래의 기회를 확보하고 문제점을 최소화 시키며 디지털시대에 부합하려는 노력의 일환으로 이해되고 있다.

Ⅱ. 기존 EU Data Protection Directive 개정 필요성

2.1 개인 기본권 강화 필요성

현재의 DPD가 적용되어 왔던 과거 17년 동안 Social networking과 같은 새로운 방식의 개인정보를 공유하는 커뮤니케이션이 등장했고, Cloud computing으로 인해 더 많은 데이터가 개인 각자의 PC가 아닌 원격지의 대용량 서버/스토리지에 저장되고 있다. 유럽에서만 적어도 2억 5천만 명 이상이 인터넷을 사용하며, 빠르게 변화하는 온라인 환경에서 개인은 각자 자신의 개인정보에 대해 효과적인 통제를 확보해야 하는 처지에 놓여 있고, 이것은 인간의 기본적인 권리이며 반드시 보호되어야 한다는 것이 과거에서 현재까지 공유되는 원칙이었다. 개선된 개인정보보호 법률은 개개인이 자신의 개인정보가 특히 온라인에서 어떻게 다뤄지는 지에 대해 확신을 줄 수 있으며, 온라인 서비스에 있어서 더욱더 강한 신뢰관계를 조성하여 신기술을 보다 안전하게 사용하게 한다. 새롭고, 명확 및 확고한 법률은 안전한 개인정보보호 프레임워크 하에서 데이터의 자유로운 소통을 가능하게 한다. 결국, 이는 양질의 제품과 서비스를 이전보다 낮은 가격에 접할 수 있다는 시장의 기본적인 기능을 강화하게 한다.

2.2 Social Networking 대응 필요성

Social networking은 친구, 가족 및 동료와 관계를 유지시키도록 유용한 도구를 제공하는 반면에, 개인정보, 사진, 댓글 등에 대해 사용자가 인식하지 못하는 범위/대상에 대한 노출 리스크가 존재한다. EU회원국 국민을 대상으로 한 Survey에서 응답자 3분의 1 이상이 현대사회에서 개인정보의 제공 등이 불가피하다고 생각하

* sangwookim@outlook.com

는 동시에 72% 이상이 과도한 개인정보 제공 등에 대해 우려하고 있다고 답변하고 있다.

2.3 국제협력 촉진 필요성

국가간의 개인정보의 이전(transfer)과 저장(store)은 Cloud computing의 확산으로 인해 이전과 비교하여 기하급수적으로 늘고 있고 이러한 데이터 흐름의 글로벌화는 당연히 개인정보보호 강화 필요성을 요구하게 한다. 이러한 요구사항은 글로벌 환경에서의 손쉬운 개인정보의 이전/저장과 함께 불필요한 복잡성과 허점이 최소화된 일관되고 높은 수준의 개인정보보호를 위한 강력한 원칙을 포함하고 있다.

2.4 시장기능 활성화 필요성

현재의 DPD는 27개 EU회원국 별로 상이한 법률 적용으로 인한 문제점을 도출하고 있다. 예를 들어, EU 내에서 비즈니스를 영위하는 어떤 글로벌 기업은 최다 27개의 개인정보보호 관련 컴플라이언스를 다룰 수도 있다는 의미이다. 이렇게 회원국 별로 개별적으로 적용되는 법률체계는 법적 불명확성 및 개인정보보호의 불균등성을 유발하며, 나아가서 기업에 있어 불필요한 비용 및 심각한 장애물로 대두 될 수 있다는 리스크가 있다. 이러한 복잡한 생태환경은 기업(특히 중/소기업)이 EU내에서 사업을 확장하는데 커다란 장애물로 인식되고 있다.

2.5 기존 DPD의 단순명료화 필요성

개인과 기업은 일관된 개인정보보호 법률이 동일한 절차/방법에 의해 EU 내에서 적용되는 것을 원한다. EU회원국 국민을 대상으로 한 Survey에서 90% 이상의 응답자가 일관된 법률이 필요하다고 응답했음에도 현재의 DPD는 이를 충족시키지 못하고 있다. 이러한 기존 법률의 단순명료화의 범위에서 개정안은 연 1억 3천만 Euro로 추산되는 기업의 breach notification 관련 의무를 상당 부분 해소하게 할 것으로 예상되고 있다.

Ⅲ. EU Data Protection 개정안 주요 내용 및 이슈

3.1 Directive가 아닌 Regulation

EU Data Protection 개정을 주도하는 European Commission(이하 EC)는 앞에서 언급한 회원국 별로 상이한 법 적용으로 인한 불균등성을 해소하기 위해 기존의 Directive 체계가 아닌 Regulation 체계를 처음으로 적용했다. 이것은 일관성과 조화를 확보하기 위한 가장 강력한 방법이며, 이를 통해 Regulation은 회원국 자체 내부 법령 제정과 이에 동반되는 일종의 자체 수정 없이 EU회원국 내에서 동일하게 즉시 효력을 발휘하게 된다.

3.2 법률 효력 범위의 실질적인 확장

개정안은 기존의 DPD가 controller(주로 기업)의 또는 개인정보 데이터를 처리하는 시설의 위치에 그 사법권을 해석했던 것에 비해, 개정안 Recital 15에서 EU에 거주하는 Data Subject(주로 고객, 개인)에 “directed to” 또는 “serves to monitor the behaviour”라는 용어를 사용하여 그 법적 범위를 확장하고 있다, 이는 EU회원국 국민을 대상으로 비즈니스를 수행하고 개인정보를 수집/처리하는 non-EU Controller(주로 외국계 기업)에게 심각한 영향을 주며, 실제적으로 EC 등의 개인정보보호 관련 기관에 대응하기 위한 대표자 등을 선임하고 유지해야 하는 의무로 나타나고 있다.

3.3 명확하고 세분화된 consent 요구사항

개정안은 기존의 전반적인 개인의 동의가 아닌 개별적인 사안 및 목적 별로 명확하고 세부적인 동의(Consent)를 확보하도록 요구하고 있다. 이는 결국 기업이 기존의 방식대로 consent 요구시스템을 유지 할 경우 의도한 동의 확보가 용이하지 않도록 만들고 있다.

3.4 개인정보보호 신개념 등장

3.4.1 Right to be forgotten

개인(Data Subject)은 기업(Data Controller)에게 그

들의 개인정보 수집/처리 등에 대한 동의(Consent) 철회 시 개인정보를 더 이상 저장하지 않고 삭제하라는 정당한 요구를 하고, 기업은 이에 따라 삭제하도록 하는 내용이 개정안에 새롭게 포함되어 있다. 특히, 개정안은 사회적 약자(Minor)-어린이, 노인, 장애인 등-의해 제공되는 개인정보에 대해 이러한 새로운 권리가 강력한 효력을 발휘할 것으로 예상하고 있다.

3.4.2 Privacy Impact Assessment

기업(Controller, Processor)은 개정안에 의해 특별히 개인의 민감한 정보 처리 이전에 Privacy Impact Assessment를 수행하도록 요구되고 있다.

3.4.3 Privacy by Design/Default

개정안은 “Privacy by Design/Default”의 개념을 포함한 원칙을 기업들이 준용하도록 포함하고 있다. 이는 첫째로 기업은 적절한 technical, organizational 통제와 절차를 구현하여 개인정보 처리 시 적용되도록 하고, 둘째로, 기본적으로 수집된 개인정보가 의도된 목적에 대해서만, 최소한의 기간 안에서 사용/처리되도록 해야 한다는 원칙이다. 즉, “Privacy by Design”은 개인정보를 수집 및 처리하기 위한 기업의 정책, 절차 및 시스템 등은 Regulation에서 제시하는 요구사항을 기본적으로 충족 시킬 수 있도록 설계 및 운영되어야 한다는 것이다. 더불어, “Privacy by Default”는 기업이 개인에게 제시하는 개인정보 관련 configuration이 default 상태-즉, 개인/고객이 자의적 선택을 하지 않았을 경우-가 가장 강력한 Privacy 수준을 확보할 수 있도록 정의되어 있어야 한다는 의미이다.

3.4.4 Data Portability

개인은 그들의 개인정보의 복사본을 기업으로부터 “널리 사용되는 구조화된 포맷”으로 제공 받을 수 있고, 이를 기업의 승인 등과 관계 없이 언제든, 어디로 이동시킬 수 있는 권리가 있다. 예를 들면, A기업 온라인 서비스를 이용하기 위해 상세한 개인정보를 제공했던 Joe Bloggs씨가 더 나은 서비스를 제공하는 B기업 온라인 서비스 가입 및 개인정보 제공을 위해 A기업에게 자신의 개인정보를 “널리 사용되는 구조화된 포맷”으로 B기업으로 이동시키도록 요구할 수 있다는 것이다.

3.4.5 One-stop-shop

기존에 개별적으로 대응해야 했던 EU회원국 별 개인정보보호 법률이 아닌 Regulation의 형태로 EU내에서 비즈니스를 영위하는 EU 또는 Non-EU 기반 글로벌 기업은 개정안이 제시하는 법률의 Requirement에 대해서만 의무를 가진다. 또한, EU내 에서 글로벌 기업의 Headquarter가 존재하는 회원국의 개인정보보호 관련 기관의 감사 등에 대해서만 대응하게 되면 다른 Subsidiaries가 존재하는 타 회원국의 개인정보보호 관련 기관에 대한 대응을 불필요하게 된다. 예를 들면, 영국에 유럽본부가 있고, 법인이 독일, 프랑스, 이탈리아에 있는 글로벌 기업 A는 새로운 개정안 하 에서는 영국의 개인정보보호 관련 기관인 ICO(Information Commissioner's Office)의 관련 대응만 하게 되면, 본부 이외의 법인이 위치하고 있는 독일 등의 국가에서는 관련 기관 대응이 면제된다고 해석할 수 있다.

3.4.6 International Transfer

주관기관인 EC의 “Adequacy” 범주에 해당하는 어떠한 Non-EU 국가와 EU회원국 국민의 개인정보의 이동/저장을 허가한다는 의미이다. 2012년 10월 현재 미국, 호주, 캐나다, 아르헨티나, 우루과이 등의 총 12개국이 이러한 Adequacy 지위를 확보하여 개인정보의 국제적 이동에 대해 상대적으로 자유로운 상황이다. 추가적으로, GE(General Electric)과 같은 글로벌 기업들은 위에서 언급된 국가별 Adequacy list가 아닌 기업에게 유사한 권리를 부여하는 BCR(Binding Corporate Rules) Scheme 하에서 GE 내에서의 EU회원국 국민의 개인정보의 자유롭고 안전한 이동 및 저장에 대해 승인을 받고 있는 상황이다.

Ⅳ. 결론 및 시사점

지금까지 과거 17년 동안 존재했던 DPD가 개인 기본권 강화, Social Networking등의 새로운 기술 대응, 국제협력 촉진과 시장기능 활성화, 그리고 기존 DPD의

단순명료화 필요성 등에 의해 Regulation의 형태로 EU 회원국 국민의 개인정보를 처리하는 글로벌 기업에게까지 법률적 효력 범위를 실질적으로 확장하고, 세부적으로 명확하고 세분화된 consent 요구사항과 Right to be forgotten, Privacy by Design/Default 등의 개인정보보호 관련 신개념을 개정안에 포함시키는 노력 등을 전체적으로 조망해 보았다.

이러한 변화는 수출 의존도가 높은 대한민국의 주요 기업들 - 특히 EU내에서 비즈니스를 확장하는 기업- 개인정보보호 컴플라이언스가 더 이상 현지 법률 회사의 간략한 검토 등의 의해 해결되는 단순한 사안이 아닌 기업 내부의 정책, 절차 및 프로세스와 이를 지원하는 인프라 및 비즈니스 시스템의 전반적인 검토와 법률에 부합하는 수정 및 보완 등이 절실히 요구된다 하겠다.

참고문헌

[1] Birnhack, M.D., 'The EU Data Protection Directive: An engine of a global regime', Computer Law and Security Report, 24, pp. 508-520, 2008.

[2] Eecke, P., Craig, C., and Halpert, J., 'The first insight into the European Commission's proposal for a new European Union Data Protection Law', Journal of Internet Law, pp. 19-22, 2012.

[3] Gilbert, F., 'Proposed EU Data Protection regulation: The Good, The Bad and The Unknown', Journal of Internet Law, 15(10), pp. 20-34, 2012.

[4] http://ec.europa.eu/justice/data-protection/document/index_en.htm.

〈著者紹介〉

김 상 우 (Kim, Sang Woo)
종신회원

2000년 2월: 중앙대학교 산업정보학과 학사
2000년~2001년: 펜타시큐리티시스템/마크로테크놀러지, Senior Consultant
2002년~2010년: Deloitte, Security & Privacy services, Senior Manager
2012년 9월: Royal Holloway, University of London, MSc in Information Security
<관심분야> 정보보호관리, 개인정보보호, Governance, Risk and Compliance, IT Risk/Audit 등