情 報 保 護 學 會 誌
第23卷 第1號, 2013. 2

글로벌 프라이버시 원칙 비교분석

염 흥 열* , 고 재 남**

요 약

최근 들어 개인정보 유출 사고가 빈번히 발생하고 있어, 개인정보 보호를 위한 법제도적 대책뿐만 아니라 기술적 보호대책의 강화가 요구되고 있다. 그러나 국가마다 지역마다 서로 다른 개인정보보호관련 법 제도적 요구사항의 상이는 서로 다른 보호조치 수준을 초래하며, 이는 궁극적으로 국가 간 또는 지역 간 개인정보의 자유로운 이전의 커다란 장애물이 되고 있다. 따라서 글로벌하게 합의된 프라이버시 원칙이 요구되었으며, 이에 기반을 둔 보호대책(control)의 개발이 필요하게 되었으며, 이 보호대책은 기업에 의해 수립되는 개인정보보호관리체계 (PIMS, personal information management system)의 인증 기준이 되며, 개인정보관리체계의 인증은 국가간 개인정보보호의 원만한 이동을 가능케 할 것이다.

본 논문에서는 각각 경제협력개발기구(OECD), 아시아태평양경제협력기구(APEC), 그리고 국제표준화 기구인 ISO/IEC, 그리고 한국 정보통신기술협회(TTA) 정보통신단체표준에서 정의된 프라이버시 원칙을 살펴보고, 각 프라이버시 원칙을 비교한다. 또한, 최근 구글의 개인정보통합관리에 대응할 수 있는 비연결성(unlikability) 원칙을 포함한 추가적인 프라이버시 원칙도 제시한다. 참고로 본 논문의 내용은 TTA 표준[4] 개발 시에도 반영 되었다.

Ⅰ. 서 론

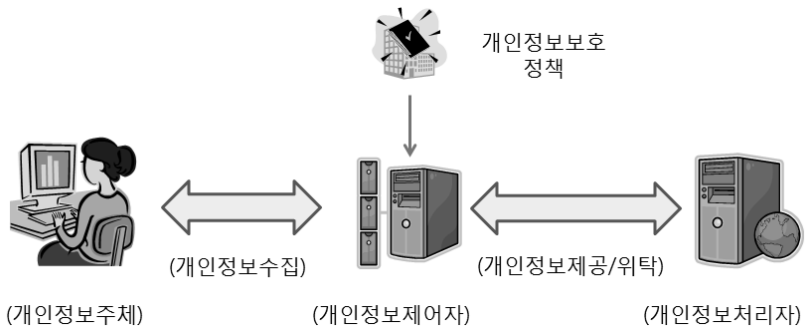
최근 들어 개인정보 유출 사고가 빈번히 발생하고 있어, 개인정보 보호를 위한 법제도적 대책뿐만 아니라 기술적 보호대책의 강화가 요구되고 있다. 그러나 국가마다 지역마다 서로 다른 개인정보보호관련 법 제도적 요구사항의 상이는 서로 다른 보호조치 수준을 초래하며, 이는 궁극적으로 국가간 또는 지역간 개인정보의 이전의 커다란 장애물이 되고 있다. 따라서 글로벌하게 합의된 프라이버시 원칙의 개발이 요구되며, 이에 기반을 둔 보호조치(control)의 개발이 필요하게 되었다. 이 보호조치는 기업에 의한 개인정보보호관리체계 (PIMS, personal information management system) 수립의 기준이 되며, 개인정보관리체계의 인증은 국가간 개인정보보호의 원만한 이동을 가능케 할 것이다.

프라이버시 보호의 경우, 보호 대상이 일반 정보가 아닌 개인정보이며, 조직이 수집해 관리하는 개인정보를 보호하는 것은 결국 정보주체의 정보 프라이버시를 보장하게 만든다.

따라서 글로벌하게 적용 가능한 프라이버시 원칙을 합의하는 것은 국가 간의 개인정보 이전을 촉진하기 위한 필요 조건이 될 수 있으며, 각 국가별 개인정보보호 법제도의 근간이 된다. 지금까지 여러 국제 기구나 표준화 기구에서는 프라이버시 보호 원칙을 개발하기 위한 논의를 진행해 왔다. 그 중에서 대표적인 프라이버시 원칙은 경제협력개발기구(OECD), 아시아태평양경제협력기구(APEC), 그리고 국제표준화 기구인 ISO/IEC 에서 정의된 프라이버시 원칙 등을 들 수 있다.

본 논문에서 이용되는 정보주체(data subject), 개인정보제어자(data controller), 개인정보처리자(data processor)와의 관계는 [그림 1]과 같다. 정보주체(data subject)는 개인정보에 의하여 알아볼 수 있는 사람으로서 개인정보의 주체가 되는 사람을 나타내며, 개인정보제어자(data controller)는 개인 정보의 처리를 위한 목

본 논문은 2012년도 방송통신위원회의 지원을 받는 방송통신표준기술력 향상 사업의 지원을 받아 수행된 표준화사업결과임. (개인정보보호관리체계(PIMS) 국제 표준 개발 No. 2012 - PK10 - 19)
* 순천향대학교 정보보호학과 교수 (hyyoum@sch.ac.kr)
** 순천향대학교 정보보호학과 학생 (freeinlove1127@gmail.com)



〔그림 1〕 개인정보관리를 위한 주요 주체들

적과 수단을 결정하는 공공기관, 법인, 단체 및 개인 등의 주요 이해 당사자이며, 개인정보처리자(data processor)는 개인정보제어자의 정책으로 개인 정보 제어자(처리자)를 대신해 개인 정보를 처리하는 주요 주체. 개인정보제어자가 될 수도 있고, 대리인 등 개인 정보 처리를 위탁 받은 자를 의미한다.

국내 개인정보보호법에서는 개인정보제어자를 개인정보처리자로 개인정보처리자는 위탁처리자로 명명하고 있으나, 본 고에서는 국제표준에서 정의되고 있는 용어를 사용했다.

본 논문에서는 주요 국제 기구의 프라이버시 원칙을 살펴보고, 국내에서 최근 표준화된 프라이버시 보호 원칙과 비교분석한다. 이를 위해 2장에서는 각 국제기구에 의해 정의된 프라이버시 원칙들을 제시하며, 3장에서는 각 국제기구에서 제시한 보호 원칙을 서로 비교하며, 4장에서는 결론을 맺는다.

Ⅱ. 본 론

2.1 OECD 프라이버시 원칙 [1]

경제협력및개발 국제기구인 OECD(Organization for Economic Cooperation and Development) 에서는 국가간 개인정보 이전을 원활하게 하기 위해 1978년부터 프라이버시 원칙에 대한 논의를 시작해, 1980년 "프라이버시 보호와 개인 정보의 국제 유통에 관한 가이드라인에 관한 이사회 권고"라는 지침(guideline)으로 채택했다. 이 지침은 공공 또는 민간 부문의 특정 정보주체와 관련된 개인 정보를 보호 대상으로 하고 있다. 즉, 프라이버시 보호, 정보의 자유로운 유통 장려, 국내 프라이버시 입법에 의한 자유로운 개인정보 유통에 대한 부당한 제한 방지, 관련 국내법 규정과의 조화를 주목적으로 하고 있다. 구체적으로, OECD 프라이버시 지침의 8대 원칙은 다음과 같이 구성되어 있다.

- 수집 제한의 원칙(Collection Limitation Principle): 개인정보의 수집에는 제한이 있어야 하고, 개인정보는 적법하고 공정한 수단으로 수집되어야 하며, 가능하면, 정보 주체의 동의와 숙지 하에 수집되어야 한다.
- 개인정보 정확성 원칙(Data Quality Principle): 개인정보는 이용 목적에 부합되면서 정확해야 하고, 완전해야 하며, 최신(up-to-date)으로 유지되어야 한다.
- 목적 명확화의 원칙(Purpose Specification Principle): 개인정보의 수집 목적은 개인정보 수집 이전에 명확화(특정)되어야 한다. 또한, 수집 이후 개인정보 이용도 해당 수집 목적으로 제한되어야 하며, 해당 수집 목적에 모순되지 않아야 한다.
- 이용 제한의 원칙(Use Limitation Principle): 개인정보는 정보 주체의 동의를 명시적으로 얻거나 관련 법령에 근거하지 않은 경우를 제외하고는 당초 수집 목적 이외 목적으로 공개, 제공, 또는 이용되지 않아야 한다.
- 안전성 확보의 원칙(Security Safeguards Principle): 개인정보는 비인가 접근, 비인가 파기, 비인가 이용, 비인가 변경, 또는 비인가 공유 등과 같은 프라이버시 위험으로부터 적절하고 합리적인 보안 대책으로 보호되어야 한다.
- 공개 원칙(Openness Principle): 개인정보에 관한 제도개선, 관행, 그리고 정책은 모든 정보주체에게

공지되어야 하며, 개인정보의 존재나 성격, 이용의 주요 목적, 그리고 개인정보제어자의 접촉 거주지와 신원을 파악할 수 있는 정보를 제공해야 한다.

- 정보주체 참여 원칙 (Individual Participation Principle): 정보주체는 다음과 같은 권한을 가져야 한다.
  - 개인정보제어자는 정보주체 개인정보를 소지하고 있는지에 대해 확인 메시지를 받을 수 있다.
  - 정보주체는 합리적인 시간 내에, 적절한 비용으로, 정보주체가 이해하기 용이한 형태로 정보주체와 관련된 개인정보를 전달 받을 수 있어야 한다.
  - 정보주체 요구가 거부되는 경우, 정보주체는 그 거절 사유를 받을 수 있어야 하며, 그러한 거절에 대해 이의를 제기할 수 있어야 한다.
  - 정보주체는 자신의 개인정보를 제어자에게 요구할 수 있어야 하고, 개인정보제어자가 관리하는 자신의 개인정보를 삭제, 보완, 수정, 변경할 수 있어야 한다.
- 책임의 원칙(Accountability Principle): 개인정보제어자는 위에서 제시된 프라이버시 원칙들이 적절히 지켜질 수 있도록 필요한 대응 조치를 구현할 책임을 져야 한다.

2.2 아시아 태평양 경제협력 기구(APEC) 프라이버시 프레임워크 [2]

아시아 태평양 경제협력 기구인 APEC은 2004년 아시아 태평양 역내 국가 간의 개인정보의 자유로운 이동을 장려하기 위한 프라이버시 프레임워크를 채택했다. APEC 프라이버시 원칙은 개인정보를 위한 적절한 프라이버시를 보호하고, 개인정보 흐름에 대한 불필요한 장벽의 생성을 막으며, 역내 다국적 기업이 개인정보의 수집, 이용, 처리의 통일되고 일관적인 접근 방법으로 구현 가능케 하며, 프라이버시 보호를 향상하고 시행하기 위한 국내 및 국제 활동을 촉진할 목적을 갖는다. APEC 프라이버시 9대 프라이버시 원칙은 다음과 같이 구성되어 있다.

- 피해 예방의 원칙: 잘못된 개인정보 수집이나 개인정보의 오용으로부터 정보주체가 피해를 입는 것을 막기 위해 고안되었고, 정보주체의 프라이버시 침해 구제 방법이 피해 위협의 가능성과 심각성에 비례하도록 규정하고 있다.
- 고지(notice) 원칙: 개인정보제어자는 개인정보를 수집할 경우 정보주체에게 제공되는 고지에서 프라이버시 정책에 관한 정보를 제공해야 하며, 실질적 고지는 수집 이전에, 또는 수집 시에, 수집 이후 가능한 빠른 시기 내에 이루어져야 한다.
- 수집 제한 원칙: 수집 제안은 수집 목적과 관련되며 필요한 경우, 정보주체의 동의와 고지 하에 합법적이고 공평하게 수행되어야 한다.
- 개인정보 이용 제한의 원칙: 개인정보 이용은 수집 목적, 호환되는 목적, 또는 관련 목적으로 제한되어야 한다.
- 선택의 원칙: 정보주체가 개인정보의 수집, 이용, 제공과 관련된 선택권을 행사할 수 있는 장치를 제공해야 한다.
- 개인정보 무결성 원칙: 개인정보는 정확하고 완전해야 하며, 비즈니스 목적에 필요한 만큼 최신으로 유지되어야 함을 제공한다.
- 보안 대책 원칙: 보호대책은 위협되는 피해의 가능성과 심각성 그리고 유지되는 환경에 비례해 개인정보 보호를 위해 적용되어야 한다.
- 접근제어 및 정정의 원칙: 정보주체는 개인정보의 접근 권한을 가져야 하며, 개인정보의 정확성에 대해 이의 제기를 할 수 있어야 하며, 필요시 개인정보의 수정을 요구할 수 있어야 한다.
- 책임성의 원칙: 개인정보제어자가 위의 원칙들에 구현할 후 있는 대책을 마련할 수 있도록 책임성을 부여해야 한다.

2.3 ISO/IEC 29100 프라이버시 원칙 [3]

2011년 채택된 ISO/IEC 29100 국제 표준에서는 11대 프라이버시 원칙을 제시하고 있다.

2.3.1 동의와 선택 원칙

동의와 선택 원칙은 최소한 다음을 만족한다.

- 개인정보 주체가 자유롭게 동의할 수 없는 경우나 관련 법령이 정보주체가 동의하지 않더라도 개인정보 처리를 허용하는 경우를 제외하고는, 정보 주체는 자신의 개인정보 처리를 허용할지 여부를 선택

할 수 있어야 하며, 정보 주체에 의한 선택은 자유롭게, 명확하게, 잘 이해 할 수 있는 방법으로 이뤄져야 한다.
- 관련 법령(applicable law)이 정보주체가 동의하지 않더라도 민감(sensitive) 개인정보의 처리를 허용하는 경우를 제외하고는, 개인정보제어자는 민감 개인정보를 처리와 수집을 위해서는 정보주체의 옵트인 (opt-in) 동의를 얻어야 한다.

2.3.2 목적 합법성과 명세성

목적 합법성과 명세성 원칙은 최소한 다음을 만족한다.
- 처리 목적은 관련 법령을 준수해야 하고 법적 근거를 가져야 한다.
- 개인정보를 수집하기 이전 또는 새로운 목적으로 처음 이용할 때마다 처리 목적은 정보주체에게 미리 알려져야 한다.

2.3.3 수집 제한

수집 제한 원칙은 최소한 다음을 만족한다.

개인정보의 수집은 관련 법령에 정해진 수집 범위 내에서 명시된 목적으로 제한되어야 한다.

2.3.4 데이터 최소화

데이터 수집 최소화는 수집되는 데이터를 최소화하는 것을 의미하지만, 데이터 최소화는 개인정보 처리를 엄격히 최소화하는 것이다. 데이터 최소화 원칙은 최소한 다음을 만족한다.
- 처리되는 개인정보는 최소화되어야 하며, 개인정보에 접근할 수 있는 이해당사자들의 수를 최소화해야 한다.
- 개인정보 처리는 공적 임무를 수행하기 위해 해당 개인정보로 접근이 허용된 개인정보처리자에게만 허용되어야 한다.

2.3.5 이용, 보유, 공개 제한

개인정보의 이용, 보유, 공개 제한의 원칙은 최소한 다음을 만족한다.
- 개인정보 이용, 보유, 그리고 공개는 명확하고, 분명하며, 합법적인 목적으로 제한되어야 한다.
- 개인정보의 이용은 개인정보제어자에 의해 수집 전에 선언된 목적으로 제한되어야 한다.

2.3.6 정확성 및 품질

정확성과 품질의 원칙은 최소한 다음을 만족한다.
- 처리되는 개인정보는 정확해야 하고, 완전해야 하며, 최신으로 유지되어야 하며, 처리는 이용 목적에 적합해야 한다.
- 정보 주체 외의 정보원(source)로부터 수집된 개인정보의 신뢰성을 보증할 수 있어야 한다.
- 정확성 및 품질을 보장하는 개인정보 수집 절차를 수립해야 한다.
- 수집되고 저장된 개인정보의 정확성과 품질을 주기적으로 검토하기 위한 메커니즘을 수립해야 한다.

2.3.7 공개, 투명, 그리고 고지

공개, 투명 그리고 고지의 원칙은 최소한 다음을 만족한다.
- 개인정보제어자의 보호 정책, 처리 과정, 관행에 대한 정보를 접근하기 쉬운 형태로 정보주체에게 제공해야 한다.
- 개인정보제어자는 정보주체에게 개인정보의 처리, 접근, 수정, 제거를 제한하기 위한 선택과 수단을 공개해야 한다.
- 개인정보 처리 과정에 중대한 변경이 발생할 때 정보주체에게 이 변경을 고지해야 한다.

2.3.8 정보주체 참여와 접근

개별 참여와 접근 원칙은 최소한 다음을 만족한다.
- 정보주체의 신원은 적정한 수준으로 인증되고 난 후, 정보주체는 자신의 개인정보로 접근할 수 있어야 하며, 검토할 수 있어야 한다.
- 정보주체는 개인정보의 정확성과 완전성에 대해 질의할 수 있어야 하며, 환경이 허용한다면, 자신의 개인정보를 개선, 정정, 삭제할 수 있어야 한다.

2.3.9 책임성

책임성 원칙의 준수는 다음을 의미한다.
- 개인정보제어자는 프라이버시 관련 정책, 절차, 그리고 관행을 적절하게 문서화하고 정보주체에게 소통해야 한다.
- 조직 내 특정 개인책임자를 개인정보관련 정책, 절차, 그리고 관행을 구현하기 위한 업무에 할당해야 한다.

2.3.10 정보보안

정보보안 원칙은 다음을 만족한다.
- 개인정보의 무결성, 기밀성, 가용성을 보장하기 위하여 적절한 통제수단으로 보호해야 하며, 개인정보 전 수명 동안 비인가된 접근, 파괴, 이용, 변경, 공개 또는 손실과 같은 위험으로부터 보호해야 한다.
- 개인정보제어자는 조직적, 물리적, 기술적 통제수단의 검토를 통해 개인정보 처리를 위임하는 개인정보처리자를 선택할 수 있어야 한다.

2.3.11 프라이버시 준수

프라이버시 준수 원칙은 최소한 다음을 만족한다.
- 내부 감사자 또는 외부 제삼자 감사기관을 통해 주기적인 감사의 실시를 통해 처리가 데이터 보호와 프라이버시 보호 요구사항을 만족한다는 것을 증명해야 한다.

2.4 국내정보통신단체표준의 프라이버시 원칙 [4]

본 절에서는 국내 정보통신기술협회의 정보통신단체표준(TTAK.KO-12.0200) 에서 제시된 프라이버시 원칙을 설명한다. TTA 정보통신 단체 표준의 프라이버시 원칙은 ISO/IEC 29100 국제 표준에서 제시된 보호 원칙과 각종 주요 국제기구의 프라이버시 원칙에 기반을 두고 있으며, 또한, 2011년 제 제정된 개인정보 보호법 [5]과 정보통신망 이용촉진 및 정보 보호 등에 관한 법 [6] 또는 관련 지침을 고려해 마련되었다.

2.4.1 피해 방지 (prevent harm)

프라이버시 보호는 개인 정보의 오용을 막도록 설계되어야 한다. 잘못된 정보 수집이나 개인 정보의 오용으로부터 정보 주체가 피해를 입는 것을 막기 위해 고안되었고, 프라이버시 침해 구제 방법과 절차가 피해 위협의 가능성과 심각성에 비례해 마련되어야 한다.

2.4.2 책임성 (accountability)

프라이버시 요구 사항을 만족해야 하는 개인정보제어자는 프라이버시 요구사항의 준수를 보증하기 위해 필요한 책임성이 있고 적절한 보안 통제를 이용해 프라이버시 정책과 절차, 그리고 관행을 시행해야 한다. 개인정보제어자는 자신의 통제 하에 있는 개인 정보를 책임져야 하며, 개인 정보 관리를 전적으로 책임질 개인정보보호책임자(CPO, Chief Privacy Officer)를 임명해야 한다. 또한, 임명된 개인 정보 보호 책임자는 프라이버시 보호 원칙을 준수하는지를 관리 감독할 책임을 져야 한다. 그리고 수립된 프라이버시 보호 원칙은 법적 관할권의 개인정보보호관련 법적 요구사항을 준수하고 지원해야 한다. 개인정보제어자는 실행 가능하고 감시 가능한 방법으로 외부적 제한 및 요구 사항에 대한 준수를 분명히 보증할 수 있는 프라이버시 정책과 절차를 수립하고 시행해야 한다. 개인정보제어자는 개인 정보 처리 업무를 대리인이나 제3자에게 위탁하는 경우, 대리인이나 제3자가 개인정보제어자에 의해 수립된 적절한 프라이버시 보호 요구사항을 완전하게 이해하고, 대리인 또는 제3자 등의 이해 당사자들이 적절한 프라이버시 요구 사항을 지원하고 준수하도록 보증해야 한다. 개인 정보 처리는 주의 의무와 확고하고 실용적인 대응 수단을 채택해 보호해야 한다. 또한 다음을 만족해야 한다.
- 프라이버시 관련 정책, 절차, 그리고 관행을 적절하게 문서화하고 소통해야 한다.
- 개인 정보를 제3자에게 전달할 때, 제3자가 계약 또는 강제 내부 정책과 같은 수단을 통해 같은 수준의 보호 수단을 의무적으로 제공하도록 해야 한다.
- 개인 정보에 접근할 수 있는 개인 정보 처리자의 임직원에 대해 적절한 교육 훈련을 제공해야 한다.
- 정보 주체의 권리 보장을 위해 효과적인 내부 고충처리와 정정 절차를 수립해야 한다.

- 정보 주체에게 피해를 줄 수 있는 프라이버시 침해와 해결을 위한 조치를 정보 주체에게 알려야 한다.
- 위험 수준에 따라서 특정 법에서 요구하는 경우 프라이버시 침해 사실에 대해 모든 관련 프라이버시 이해 당사자에게 통보해야 한다.
- 프라이버시 침해가 발생한 경우, 정보 주체(또는 정보 주체 집단)가 적절하고 효과적으로 처벌 또는/그리고 개정, 손해배상 등의 법적 구제 수단에 접근할 수 있도록 해야 한다.
- 정보 주체의 프라이버시 상태가 사건이 발생하지 않은 상태로 복귀하는 것이 어려운 상황에 대한 보상 절차를 고려해야 한다.

2.4.3 목적 합법성과 명세성 (purpose legitimacy and specification)

개인정보의 수집 목적은 개인정보 수집 이전에 명확화(특정)되어야 한다. 수집 이후 개인정보 이용은 해당 수집 목적으로 제한되어야 한다. 개인정보가 수집되는 특정한 목적은 수집 당시나 수집 이전에 개인정보제어자에 의해 확정되어야 한다. 또한 다음을 보장해야 한다.

- 수집 목적은 관련 법령을 준수해야 하고 법적 근거를 자져야 한다.
- 개인정보를 수집하기 이전 또는 새로운 목적으로 다시 이용할 때 수집 목적은 정보 주체에게 알려져야 한다.
- 만약 가능하다면, 민감 개인 정보 처리 필요성에 대해 정보 주체에게 충분히 설명해야 하며, 별도의 동의를 받아야 하며, 수집 이용에 제한을 두어야 한다.

2.4.4 숙지 후 동의와 선택 (well-informed consent and choice)

개인정보제어자는 정보 주체에게 개인정보를 제공할 것을 요청하는 경우, 개인 정보의 수집과 이용이 정보 주체에게 잘 알려져야 하고 명시적 동의를 얻어야 하며 특정 수집 및 이용 목적과 연관되어야 한다. 개인 정보의 제2차 이용 또는 목적 외 이용은 정보 주체로부터 분명하고 잘 알려진 별도의 동의를 요구해야 한다. 개인의 분명하게 잘 알려진 동의나 법령에 의해 요구되는 경우를 제외하고는, 개인 정보는 수집 당시의 목적 이외의 다른 목적으로 이용되거나 제공(공유 포함)되어서는 안 된다. 또한 다음을 보장해야 한다.

- 정보 주체가 자유롭게 동의할 수 없는 경우나 다른 법률에 따라 정보 주체가 동의하지 않더라도 개인 정보 처리를 허용하는 경우를 제외하고는, 정보 주체에게 자신의 개인 정보 처리를 허용할 지 여부를 선택할 수 있어야 하며, 정보 주체에 의한 선택은 자유롭게, 명확하며, 쉽게 이해 할 수 있는 방법으로 제공되어야 한다.
- 법률에서 민감 개인정보의 처리를 허용하거나 요구하고 있는 경우를 제외하고는 민간 개인 정보를 수집 이용하기 위해서는 정보 주체로부터 별도의 동의를 받아야 한다.
- 관련 법령(applicable law)이 정보 주체가 동의하지 않더라도 고유식별정보 처리를 허용하는 경우를 제외하고는, 고유식별정보의 처리와 수집을 위해서는 정보 주체의 옵트인(opt-in) 동의를 얻어야 한다.
- 동의를 얻기 전에 정보 주체에게 개인 참여와 접근 원칙에서 제공하는 정보 주체의 권한을 알려야 한다.
- 동의를 얻기 전에, 정보 주체에게 공개, 투명, 고지 원칙에서 제시된 정보를 제공해야 한다.
- 정보 주체에게 동의하지 않는 결과에 대해 잘 알려야 한다.

2.4.5 수집 제한 (collection limitation)

개인정보의 수집은 특정된 목적과 연관되어야 하고 필요한 경우로만 한정되어야 한다. 개인 정보의 임의의 수집은 합법적이고 공정해야 한다. 개인 정보의 수집에는 제한이 있어야 하고, 개인 정보는 적법하게 공정한 수단으로 정보 주체의 동의와 숙지 하에 수집되어야 한다.

2.4.6 이용, 공개, 보유 제한 (use, disclosure, retention limitation)

개인정보는 정보주체의 동의를 얻거나 관련 법령에 근거하지 않은 경우를 제외하고 당초 수집 목적 외로

공개, 제공, 이용, 보유하지 않아야 한다. 개인 정보의 목적 외 이용과 파생 이용은 허용되지 않아야 한다. 특정 목적으로 개인 정보를 수집하고 있는 조직이 관련된 개인 정보를 다른 목적으로 이용하기를 원하는 경우, 개인정보제어자는 관련 정보 주체로부터 새롭게 직접적이며 잘 공지된 방법으로 별도의 동의를 얻어야 한다. 개인정보제어자는 개인정보를 규정된 목적을 만족하기 위해 필요한 기간 동안만 보유되어야 한다. 개인정보제어자는 정보 주체에게 개인 정보 보유 기간을 알려야 한다. 또한 다음을 제공해야 한다.

- 개인 정보의 이용, 보유, 제공(공개 포함)을 명확하고, 분명하고, 합법적인 목적을 만족하기 위해 필요한 개인 정보만으로 제한해야 한다.
- 관련 법령이 다른 목적을 분명하게 명세하지 않는다면, 수집 전 개인 정보 제어자에 의해 정의된 이용 목적으로만 개인 정보의 이용을 제한해야 한다.
- 수집 이용 목적을 달성하기 위하여 필요한 기간만 개인 정보를 보유해야 하며, 그 이후에는 개인 정보를 파기하거나 익명화해야 한다.
- 개인 정보 처리 목적을 달성하였으나 다른 법령에 따라 보유해야 하는 경우, 해당 정보는 별도로 보관하여야 한다.

2.4.7 정확성 및 품질 (accuracy and quality)

개인정보는 수집되는 목적을 위해 필요하기 때문에 정확해야 하고, 완전해야 하며 최신성을 유지해야 한다. 또한 다음을 보장해야 한다.

- 개인 정보 처리 전에 정보 주체 이외 정보 제공자(source)로부터 수집된 개인 정보의 신뢰성을 확인하고 보증해야 한다.
- 개인 정보를 변경하기 전에 정보 주체의 요구 타당성과 정확성(변경이 적절하게 허가되었다는 것을 보증하기 위해)을 적절한 수단을 이용해 검증해야 한다.
- 정확성 및 품질을 보장하도록 하는 개인 정보 수집 절차를 수립해야 한다.
- 수집되고 저장된 개인 정보의 정확성과 품질을 주기적으로 검토하기 위한 통제 메커니즘을 시행해야 한다.

2.4.8 정보 보안 (information security)

개인정보는 운영 절차나 보호 조치에 의해 보호되어야 한다. 개인정보 민감도 수준에 적합한 보호 조치와 프라이버시 보호 요구 사항을 갖는 준수를 지원하는 보호 조치를 시행해야 한다. 개인 정보는 비인가 접근, 비인가 파기, 비인가 이용, 비인가 변경, 또는 비인가 공유 등과 같은 위험으로부터 적절한 보안 대책으로 보호되어야 한다. 또한 다음을 보증해야 한다.

- 개인 정보의 무결성, 기밀성, 가용성을 보장하기 위하여 운영적, 기능적, 전략적 수준에서 개인정보를 적절한 보호수단으로 보호해야 하고 전 개인 정보 수명 동안 비인가 접근, 비인가 파괴, 비인가 이용, 비인가 변경, 비인가 공개 또는 손실 등과 같은 프라이버시 위험으로부터 보호되어야 한다.
- 개인정보 처리를 위해 조직, 물리, 기술적 통제 수단 측면을 충분히 보증하는 개인정보처리자를 선택해야 하며 적절한 보안 통제(control)로 법 준수를 보증해야 한다.
- 보안 통제들은 준거 법적 요구 사항, 보안 표준, 체계적 보안 위기 평가의 결과, 그리고 비용/혜택 분석 결과에 준거해야 한다.
- 잠재적인 결과의 심각성과 발생 가능성, 민감도, 영향 받는 정보 주체의 개수, 그리고 보유한 환경에 비례해 통제 수준을 구현해야 한다.
- 개인 정보 접근을 자신의 업무를 수행하기 위해 접근이 필요한 개인으로만 제한해야 한다.
- 프라이버시 위험 평가와 감사 프로세스를 통해 발견된 위험이나 취약성을 해결해야 한다.
- 보안 통제는 주기적으로 검토해야 하고 진행 중인 보안 위험 관리 프로세스로 재평가가 되어야 한다.

2.4.9 데이터 최소화 (data minimization)

데이터 최소화는 수집 최소화 원칙과 연결된다. 개인정보 처리 과정에서 수집 최소화는 수집되는 데이터를 최소화하는 것을 의미하지만, 데이터 최소화는 개인 정보 처리를 엄격히 최소화하는 것이다. 데이터 최소화 원칙의 준수는 데이터 처리 과정을 다음을 위해 데이터 처리 과정과 정보 시스템을 설계하고 구현하는 것을 의미한다.

- 처리되는 개인 정보와 개인 정보가 공개되고 접근되는 이해 당사자와 취급 기관의 수를 최소화해야 한다.
- 처리 최소화는 '반드시 필요한 것만 알려주는(일명, need-to-know)' 원칙이 적용되어야 한다. 다시 말해, 개인 정보 접근은 개인 정보 처리의 합법적 목적 내에서 공적 업무를 수행하기 위해 필요한 개인 정보로만 부여되어야 한다.
- 정보 주체의 식별이 어렵게 하고 이용자 행태의 가시성을 줄이며 수집된 개인 정보의 상호 연결성을 제한하는 상호 작동과 처리를 디폴트 선택으로 제공해야 한다.
- 처리 목적을 달성하였거나, 법적 보유 기간이 경과한 경우, 해당 개인 정보는 지체 없이 파기하여야 한다.

2.4.10 공개, 투명, 고지 (openness, transparence, and notice)

개인정보제어자는 정보 주체 관리와 관련된 정책과 규칙, 개인 정보의 제공에 관한 정보를 정보 주체에게 제공해야 한다. 개인 정보에 관한 제도 개선, 관행, 정책은 일반 정보 주체에게 공개되어야 하며, 처리되는 개인정보의 존재나 성격, 주요 이용 목적, 그리고 개인정보 제어자의 연락처와 신원을 알 수 있는 절차를 마련해야 한다. 또한 다음을 보장해야 한다.

- 개인정보 처리에 대한 개인정보제어자의 정책, 처리 과정, 관행에 대해 쉽고 접근하기 쉬운 정보를 정보 주체에게 제공해야 한다.
- 개인 정보가 처리되고 있다는 사실, 개인 정보가 공개되는 주요 이해 당사자들, 처리 목적, 그리고 개인 정보 제어자의 신원 정보를 고지(notice)에 포함해야 한다,
- 개인정보제어자는 목적으로 정보 주체에게 정보의 처리, 접근, 수정, 제거를 제한할 수 있는 선택과 수단을 알려야 한다.
- 개인 정보 처리 과정에서 발생하는 중대한 변경을 정보 주체에게 고지해야 한다.

2.4.11 정보주체 참여와 접근 (individual participation and access)

정보 주체는 개인정보제어자가 자신에 대한 개인 정보를 보유하고 있는지에 대해 알 권리를 보유한다. 개인정보제어자는 정보 주체의 요구 시에 해당 정보 주체에게 개인 정보의 존재, 이용, 공유(제공)에 대해 통지해야 한다. 개인정보제어자는 정보주체의 개인정보를 보유하고 있는 경우, 해당 정보 주체의 개인 정보에 대한 완전한 접근 권한을 제공해야 한다. 또한 다음을 보증해야 한다.

- 정보 주체의 신원이 적절하게 먼저 인증되고 그러한 접근이 관계 법령에 의해 금지되지 않은 경우에 해당 정보 주체에게 개인 정보로 접근하고 검토할 기회를 부여해야 한다.
- 개인 정보의 정확성과 완전성에 대해 질의가 가능해야 하며 정보 주체가 자신의 개인 정보를 개정, 정정, 삭제할 수 있어야 한다.
- 개인정보제어자는 개인 정보의 개정, 정정, 삭제 사실을 개인 정보가 제공된 개인 정보 취급 기관 또는 제3자에게 제공되어야 한다.
- 정보 주체가 이러한 권한을 쉽고, 신속하고 효과적인 방법으로 행사할 수 있는 절차를 수립해야 한다.
- 정보 주체는 자신의 개인 정보의 정확성과 완전성에 대한 시험을 할 수 있어야 하며 수정하거나 부적절한 경우 파기할 수 있어야 한다.

2.4.12 프라이버시 준수 (privacy compliance)

프라이버시 준수 원칙의 준수는 다음을 의미한다.

- 내부 감사자 또는 외부 제3의 감사 기관을 통해 주기적인 감사 실시를 통해 개인 정보 처리가 프라이버시 보호 요구 사항을 만족한다는 것을 검증하고 증명해야 한다.
- 관련 법령을 준수하고, 보안, 데이터 보호, 프라이버시 정책, 그리고 절차에 준수를 보증하기 위한 적절한 내부 통제와 독립적인 감사 메커니즘이 시행되도록 해야 한다.
- 프로그램과 서비스 전달이 데이터 보호와 프라이버시 요구 사항을 준수하고 있는 지를 평가하기 위해 프라이버시 위험 평가를 개발하고 유지해야 한다.

〔표 1〕 개인정보보호 원칙 비교

원칙 항목	TTAK.KO-12.0200	OECD	APEC	ISO/IEC 29100
피해방지	피해방지	-	피해 예방	
책임성	책임성	책임성	책임성	책임성
목적 합법성과 명세성	목적 합법성과 명세성	목적 명확화		목적 합법성과 명세성
숙지후 동의와 선택	숙지후 동의와 선택		선택	동의와 선택
수집 제한	수집 제한	수집 제한	수집 제한	수집 제한
이용, 공개, 보유 제한	이용, 공개, 보유 제한	이용 제한	이용 제한	이용, 보유, 공개 제한
정확성 및 품질	정확성 및 품질	정확성	무결성	정확성 및 품질
정보보안	정보보안	안전성 확보	보안 대책	정보보안
데이터 최소화	데이터 최소화			데이터 최소화
공개, 투명, 고지	공개, 투명, 고지	공개	고지	공개, 투명, 고지
정보주체 참여와 접근	정보주체 참여와 접근	정보주체 참여	접근제어/정정	정보주체 참여와 접근
프라이버시 준수	프라이버시 준수			프라이버시 준수

Ⅲ. 프라이버시 원칙 비교 분석 및 부가 원칙

3.1 프라이버시 원칙 비교 분석

본 절에서는 2장에서 제시된 다양한 보호 원칙을 비교분석한다. 비교 분석 결과는 [표 1] 과 같다.

3.2 기타 프라이버시 보호 원칙

기존 국제기구에서 제시된 프라이버시 원칙에는 포함되지 않았지만, 개인정보보호를 위해 추가적으로 고려해야 할 다음과 같은 원칙이 존재한다.

3.2.1 비연결성 (unlinkability) 원칙

비연결성은 개인정보가 여러 다른 프라이버시 도메인에 걸쳐서 서로 연결해 사용할 수 없으며 원래 의도된 목적 이외로 사용될 수 없음을 의미한다. 비연결성은 서로 구분된 데이터와 처리를 목적하고 있다. 이 프로세스는 개인정보가 도메인 밖 관련 개인정보와 서로 연결될 수 없도록 동작되어야 함을 의미한다.

3.2.2 개입가능성 (Intervenability) 원칙

개입가능성은 정보 주체, 정보시스템 운영자, 감독기관이 모든 개인정보 처리에 관여할 수 있도록 보장하는 것이며, 모든 당사자들이 기존 및 향후 데이터 처리에 관여할 수 있을 가능성을 제공하는 것이며, 보호대책을 수정하는 것을 적용해야 한다.

Ⅳ. 결 론

본 고에서는 국제기구에서 제시된 대표적 프라이버시 보호 원칙을 제시했으며, TTA 정보통신단체표준에서 제시된 보호원칙과 각 국제기구에서 제시된 프라이버시 원칙을 비교했다.

본 고에서 제시된 원칙은 개인정보관리체계의 수립을 위한 인증기준이 되는 보안통제를 개발하는데 유용하게 활용될 수 있다.

본 논문은 TTA 과제의 연구 결과에도 활용되었다.[4]

참고문헌

[1] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, 1980
[2] APEC, APEC privacy framework, APEC, 2004
[3] ISO/IEC 29100(2011), Information technology – Security techniques – Privacy framework
[4] TTA, TTAK.KO-12.0200(2012), 개인 정보 관리를 위한 프라이버시 보호 원칙
[5] 개인정보보호법, 2011
[6] 정보통신망이용촉진 및 정보보호 등에 관한 법, 방통위

〈著者紹介〉

염흥열 (Heung-Youl YOUM)
종신회원

한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장, 수석부회장(역), 학회장(2011), 명예회장(현)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 (구) 정통부 정보보호 PM/정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜

고 재 남 (Jae-Nam KO)

순천향대학교 정보보호학과 재학
2012년 6월~현재 : 정보보안산업표준포럼(KISSF) 제도분과 회원
<관심분야> 개인정보보안, 인터넷 보안, 홈 네트워크 보안