유럽사법재판소 세이프 하버 협정 무효 판결과 개인정보보호 정책의 변화

최경진 · 가천대 법학과 교수

초연결사회로의 전환을 가져올 제4차 산업혁명을 맞고 있는 상황에서 글로벌 네트워크를 통해 유통되는 개인정보는 초연결혁명을 이끄는 핵심 요소 중의 하나이다. 이에 선진 각국은 개인정보의 다각적인 활용을 통한 산업의 발전을 꾀하면서도, 자국 국민의 기본적 권리의 보장이라는 측면에서 개인정보를 보호하기 위한 노력도 함께하고 있다. 특히 최근 초연결혁명을 이끌고 있는 미국의 글로벌 기업을 중심으로 한 개인정보의 자유로운 활용 요구와 EU를 중심으로 한 개인정보보호 강화 노력이 강력하게 충돌하고 있다. 이런 흐름 속에서 EU의 개인정보보호 노력에 힘을 실어준 계기가 된 것이 스노든 사건이다. 또, 유럽사법재판소(European Court of Justice)의 소위 '잊힐 권리(Right to be forgotten)'와 관련된 구글 스페인 판결을 통해서도 개인정보보호의 필요성을 재확인할 수 있었다.[1] 이러한 일련의 과정을 통해 EU는 EU 회원국 전역에서 일관된 개인정보보호 수준을 확보하기 위해 추진해 온 개인정보보호규정안[2]의 입법화 작업에 가속도를 붙였다. 그리고 2015년 10월 유럽사법재판소가 미국과 EU의 개인정보 유통에 관한 안전망 역할을 해 온 세이프 하버 협정(Safe Harbor Agreement)에 대해

1) Case C–131/12, Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez (May 13, 2014).

2) 개인정보보호규정안의 최초안은 "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)", COM(2012) 11 final (Jan. 25, 2012), http://ec.europa.eu/justice/data–protection/document/review2012/com_2012_11_en.pdf (검색일: 2016. 3. 1.)

무효를 선언하면서, EU는 미국이 EU의 강화된 개인정보보호 기준을 수용하도록 압박 수위를 높이게 되었다. 결과적으로 미국과 EU는 기존의 세이프 하버 협정을 대신하는 소위 'EU-US 프라이버시 보호막(EU-US Privacy Shield)'을 채택하기에 이르렀다. 미국과 EU의 개인정보보호에 관한 공방은 우리가 향후 글로벌 무역 거래와 협상을 함에 있어서 우리 개인정보보호의 수준을 어떻게 가져가야 할 것인지에 대해 많은 시사점을 제공해준다. 이러한 관점에서 세이프 하버 협정 무효화 판결에 대해 상세히 살펴보고자 한다.

1. 세이프 하버(Safe harbor) 협정이란?

미국은 EU와의 무역 장벽을 제거하기 위해 EU가 제시하는 개인정보보호기준을 준수하는지의 여부를 판가름하는 기준으로서 7가지 항목의 세이프 하버 원칙을 제시하였다. 이 원칙을 충족하는 미국 기업은 EU 기준에 적합한 수준의 개인정보보호를 하는 기업으로 간주되어 아무런 제재 없이 EU와 개인 데이터를 이전할 수 있다. 이 원칙은 1998년 11월 4일 초안이 발표된 이후 5차례 수정을 거쳐 2000년 5월 31일 EU 회원국의 만장일치로 그 내용이 승인되었으며, 2000년 6월 9일 최종안이 발표되었다. 세이프 하버 원칙의 내용은 다음과 같다.

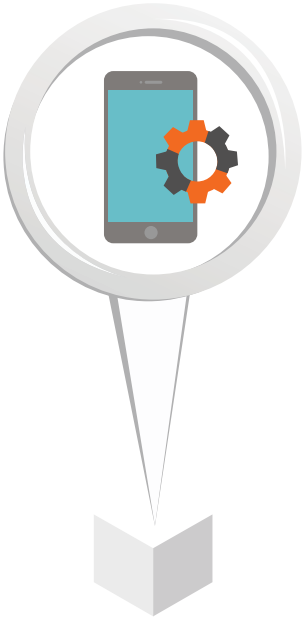
(1) 고지 (Notice)

최초 정보수집 시 또는 그 후 가능한 빨리 통지하여야 한다는 원칙을 의미한다. 그러나 최초 수집 목적 이외의 용도로 사용하는 경우 또는 최초로 제3자에게 정보를 공개하는 경우에는 반드시 사전에 통지하여야 한다.

(2) 선택 (Choice)

개인정보의 제3자에 대한 공개, 최초수집 목적 외 이용의 경우에는 정보주체에게 그에 대한 선택의 기회를 제공하여야 한다. 일반적으로는 사후 철회(opt-out) 방식을 취할 수 있지만 민감한 정보의 경우 사전 동의(opt-in) 방식을 채택하여야 한다.

(3) 제공 (Onward Transfer; Transfers to Third Parties)



제3자에게 정보를 공개하는 경우 통지 및 선택에 관한 원칙을 따라야 한다. 개인정보처리자는 대리인으로 활동하는 제3자에게 정보를 전송하고자 하는 경우, 그 제3자가 세이프 하버 원칙에 가입하였거나 EU 지침 혹은 기타 적절한 방법을 준수하거나, 최소한 세이프 하버 원칙의 관계조항이 요구하는 정도와 동일한 프라이버시 보호를 제공한다는 서면협정을 그 제3자와 체결하여야 한다. 또한 제3자가 이러한 요건을 충족한다면, 개인정보처리자는 제3자가 제한사항 등에 반하여 그 정보를 처리하고 있음을 알았거나 알 수 있었거나 혹은 제3자의 처리를 방지하기 위한 적절한 조치를 취하지 않은 경우를 제외하고는, 제3자가 어떠한 제한사항 등에 반하여 그 정보를 처리하고 있는 것에 대해 책임을 지지 않는다.

(4) 안전성 (Security)

개인정보 관련 기록을 생성, 유지, 이용 또는 보급하는 자는 손실과 오용, 비인가 접근, 공개, 변경이나 파기로부터 보호하기 위한 합리적 예방조치를 취하여야 한다.

(5) 데이터 무결성 (Data integration)

개인정보는 세이프 하버 원칙에 적합하도록 사용목적과 연관성이 있어야 한다. 당초 수집 목적 또는 개개인이 허가한 목적과 양립할 수 없는 방법으로 정보를 처리할 수 없다. 정보의 원래 목적에 맞는 사용, 정확성, 완전성, 그리고 최신성을 보장하는 합리적인 조치를 취하여야 한다.

(6) 접근 (Access)

개인은 자신에 관한 정보에 접근하여 그 비용이 개인의 프라이버시에 비해 그리 크지 않고 다른 사람의 프라이버시가 손상되지 않는 범위 내에서 이를 수정하거나 삭제할 수 있어야 한다.

(7) 집행 (Enforcement)

효과적인 프라이버시 보호는 원칙의 준수 및 원칙을 준수하지 않음으로 인해 영향을 받는 개인을 위한 청구권, 원칙을 준수하지 않는 기관에 대한 제재 등을 확실히 할 수 있는 체계를 포함하여야 한다.

제재조치는 개인정보보호 원칙의 준수를 보장하기 위하여 엄격해야 한다. 또한 매년 자체 검증 보고서를 제출하지 않으면, 세이프 하버 원칙에 따르는 보호대상에서 제외된다.

2. 세이프 하버 협정의 법적 근거가 된 EU 개인정보보호지침[3]

세이프 하버 협정이 가능하게 된 배경에는 EU가 채택한 개인정보보호지침 상의 개인정보 국외이전 체계가 있다. EU의 1995년 개인정보보호지침(이하 'EU지침')[4] 전문 제57항과 제25조 제1항에 따르면, EU 회원국 국민의 개인정보에 대한 '적절한 보호 수준(adequate level of protection)'을 보장하지 않는 경우에는 제3국[5]으로 이전할 수 없도록 하고 있다. 따라서 개인정보에 대해 적절한 수준의 보호를 하는 경우에 한해서만 이전할 수 있게 된다. EU지침 제25조 제2항에 따르면 보호의 '적절성(Adequacy)' 여부는 제3국으로의 정보 이전 활동과 관련된 주변 사정에 비추어 판단되어야 하며 개인정보의 성격, 개인정보의 처리 목적과 기간, 개인정보의 최초 이전국과 최종 도착국, 제3국에서 시행되고 있는 법률규범 · 직무규정 및 보안조치 등 개인정보 이전을 둘러싼 모든 환경이 고려되어야 한다.[6] EU의 개인정보보호작업반의 적절성 평가 관련 보고서[7]에 따르면 대체로 다음과 같은 실체적 판단기준과 절차적 판단기준에 의하여 보호의 적절성을 평가할 수 있다.

3) EU의 개인정보 국외이전에 관한 상세한 사항은 최경진, "개인정보 국외이전에 관한 소고", 『법학논총』 제20집 제1호(2013), 31–63쪽 참조.

4) Directive of the European Parliament of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC.

5) 제3국이란 유럽경제영역(European Economic Area: EEA) 회원국을 제외한 그 밖의 국가를 의미한다. 따라서 EEA 회원국 간 정보이동은 제3자로의 이동으로 간주하지 않으므로 금지대상이 되지 않는다.

6) 이광현, 2010, "국경간 개인정보 이전과 보호: EU와 영국, 미국의 사례를 중심으로", 『선진상사법률연구』 제50호, 120쪽 ; 한국인터넷법학회, 2009, "개인정보 보호와 적정 활용의 조화를 위한 제도 도입 연구", 법제처, 143쪽.

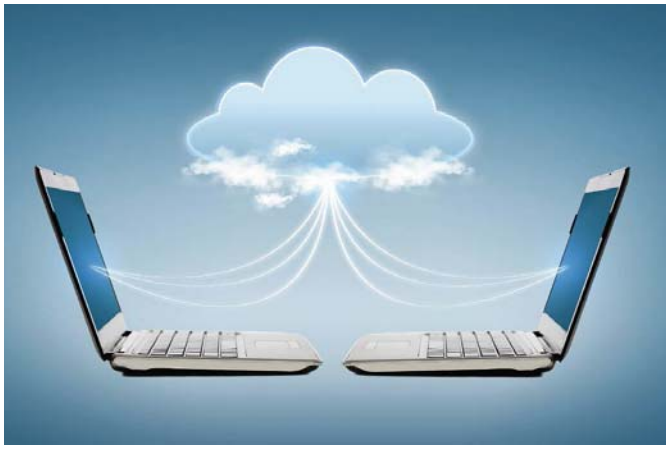
7) EU Working Party on the protection of Individuals with regard to the Processing of Personal Data, Working Document, "Transfers of personal data to third countries; Applying Articles 25 and 26 of the EU data protection directive" (1998. 7. 24)

〈실체적 판단기준〉

	기준	내용
기본 원칙	1. 목적제한의 원칙	데이터는 특정한 목적에 따라 처리되고 그 목적 범위 내에서 이용 · 제공되어야 함
	2. 정보의 질 확보 및 비례성 원칙	데이터는 정확해야 하고 필요한 경우 최신으로 업데이트되어야 함. 또한 데이터는 이전 또는 처리되는 목적에 적절하고 관련성이 있어야 하며 목적에 비해 과도해서는 안 됨
	3. 투명성 원칙	개인은 처리목적, 처리자 등 공정성을 위해 필요한 정보들을 투명하게 제공받아야 함
	4. 안전성 원칙	개인정보처리자는 적절한 기술적 · 관리적 보안조치를 하여야 함
	5. 열람 · 정정 및 반대할 권리	정보주체는 처리중인 자신에 관한 데이터의 사본을 받아볼 수 있고 부정확한 정보를 수정할 수 있으며, 자신에 관한 정보 처리를 반대할 권리를 가져야 함
	6. 개인정보의 제공 제한	1차적으로 개인정보를 제공받은 자가 다시 개인정보를 제공하는 것은 그 개인정보를 제공 받는 자도 적절한 보호수준의 원칙을 적용받는 경우에 한해서만 허용됨
추가 원칙	1. 민감정보 처리제한	민감한 정보로 분류되는 데이터는 정보처리에 대한 정보주체의 명백한 동의 등 추가적인 안전조치를 확보해야 함
	2. 다이렉트 마케팅 제한	데이터가 다이렉트 마케팅 목적으로 이전되는 경우, 정보주체는 opt-out을 할 수 있어야 함
	3. 개인에 대한 자동화된 결정 제한	개인에 대한 자동화된 의사결정을 위한 개인정보 이전의 경우, 개인은 그러한 의사결정에 사용되는 로직에 대해 알 권리가 있고 개인의 합법적 이익을 보호하기 위한 추가적인 보호조치가 취해져야 함

〈절차적 판단기준〉

기준	내용
1. 보호원칙이 잘 준수되는 체계의 확보 (good level of compliance)	개인정보처리자가 스스로의 의무를 뚜렷이 인식하고, 정보주체가 자신들의 권리 및 행사방법을 잘 알 수 있는 보호체계를 갖추어야 함. 또, 효과적이고 억제력이 강한 제재수단을 통해 보호원칙을 존중하도록 유도
2. 정보주체의 권리행사를 지원하고 도와주는 보호체계(support and help to individual data subjects)	개인이 신속하고 효과적으로, 과도한 비용부담 없이 자신들의 권리를 행사할 수 있어야 함. 이를 위해 민원 · 고충에 대한 독립적 조사가 보장되는 제도적 메커니즘 필요
3. 보호원칙 미준수로 피해를 입은 자에 대한 적절한 구제조치 필요 (appropriate redress)	손해배상이나 적절한 제재조치가 가능한 독립적 조정 또는 중재 시스템 필요



하지만 개인정보 보호 수준이 낮은 제3국으로의 개인정보 이전이 무조건 금지되는 것은 아니며, 제26조에 의해 다음과 같은 경우에는 예외적으로 개인정보보호수준이 EU의 수준에 미치지 못하더라도 제3국으로의 개인정보 이전이 허용된다.[8] ① 정보주체가 개인정보 이전에 명백히 동의한 경우, ② 정보주체와 개인정보처리자 사이에 체결된 계약의 이행에 필요한 개인정보의 이전 또는 정보주체의 요청에 따른 계약 체결 전 조치를 이행하기 위하여 필요한 개인정보의 이전, ③ 개인정보처리자와 제3자 사이에 정보주체의 이익을 위한 계약의 체결 또는 이행을 위하여 필요한 개인정보의 이전, ④ 중요한 공익적 근거에 기초하거나 소송의 제기, 수행 및 방어를 위하여 필요하거나 법적으로 요구되는 개인정보의 이전, ⑤ 정보주체의 중대한 이익 보호를 위하여 필요한 개인정보의 이전, ⑥ 개별 사안에 있어서 법률적인 조건이 충족되는 범위 내에서 공중에게 정보를 제공할 목적으로 구축되었고 동시에 공중이나 이해관계자의 상담(consultation)에 제공될 목적으로 구축된 등록부(register)로부터 개인정보가 이전되는 등의 경우에는 이전이 허용된다. 나아가 위에 열거된 경우에 해당하지 않는다고 하더라도 개인정보처리자가 개인의 프라이버시와 자유권 그밖에 이에 준하는 권리의 보호와 행사를 위해 적절한 보호 조건을 제시한 경우라면 제3국의 개인정보 보호수준이 EU 수준에 미치지 못한 경우에도 회원국은 제3국으로 개인정보 이전을 승인할 수 있다. 이 경우 개인정보처리자가 이행해야 할 개인정보의 보호조건은 계약에 의해 보증하는 것도 가능하다.[9][10] 한편, 회원국과 EU 집행위원회는 제3국의 개인정보 보호수준이 적정수준에 이르지 못한다고 판단되는 경우에는 그 사실을 다른 회원국에게 알려야 한다. 위원회는 보호수준을 높이기 위해 제3국과 협상을 추진할 수 있으며, 또한 제3국의 국내법, 제3국이 체결한 국제조약, 위원회와의 협상결과 등을 고려하여 제3국이 적절한 보호수준을 보장하고 있다고 인정할 수 있다.[11]

---

8) Directive 95/46/EC Art. 26(1)

9) Directive 95/46/EC Art. 26(2)

10) 개인정보보호를 위한 구속력 있는 기업규칙에 따른 국외이전도 허용되며, 여러 국가의 글로벌 기업들은 이러한 BCRs을 적극 활용하고자 한다. BCRs에 대한 상세 내용은 박훤일, 2005, "개인정보의 보호를 위한 안전조치 –개인정보보호 기업규칙(BCRs)을 중심으로–", 『경희법학』 제40권 제2호, 159–190쪽 참조.

11) Directive 95/46/EC Art. 25(3)~(6)

EU 지침 제25조 제6항은 EU 집행위원회(European Commission)가 개인정보에 대해서 적절한 보호를 제공하는 국가의 목록(White list)[12]을 작성할 수 있도록 규정하고 있다.[13] 다만, 예외적으로 정보이전 시 적절한 안전조치(adequate safeguards)를 마련하기만 한다면 EU 내 기업들은 적절한 보호를 제공하지 않는 외국으로 개인정보를 이전할 수도 있다. EU는 제한적으로 일부 국가에 대해서만 적절성을 판단하고 있기[14] 때문에 제25조는 현실적으로 그 의의를 상실한 반면 제26조의 유용성이 증가하면서 예외가 원칙을 지배하는 현상이 나타나고 있다.[15]

EU 이사회(European Council)와 유럽의회(European Parliament)는 EU 집행위원회에 EU지침 제25조 제6항을 기초로 제3국이 국내법이나 가입한 국제협약에 의해 적절한 보호수준을 확보하고 있는지 여부를 결정할 권한을 부여하였다. 이에 따르면 먼저 EU 집행위원회로부터 제안이 있어야 하고, 제29조 작업반의 체계 내에서 EDPS(European Data Protection Supervisor)와 각 회원국의 정보보호감독기구의 의견을 수렴하고 검토하는 절차를 거친 후 회원국의 대표로 구성되는 제31조 위원회로부터 승인을 받아 집행위원협의회(College of Commissioners)의 결정으로 채택된다. 그러나 유럽 의회와 이사회는 언제라도 집행위원회에 그 행위가 EU 지침에서 정한 실행권한을 초과하는 견지에서 적절성 결정을 유지, 수정 또는 철회할 것을 요청할 수 있다. 이러한 절차를 거쳐 적절성 결정을 받게 되면, 부가적인 안전조치 없이 28개 EU 회원국과 3개 EEA 회원국(노르웨이, 리히텐슈타인, 아이슬란드)으로부터 제3국으로 개인정보가 이전될 수 있게 된다. 그러나 이러한 적절성 결정은 법 집행 분야에서의 정보 교환은 규율하지 않는다. 따라서 해당 분야의 개인정보의 이전을 위해서는 별도의 조치가 필요하다. 예를 들면, PNR(Passenger Name Record) 협정이나 TFTP(Terrorist Financing Tracking Programme) 협정과 같은 별도의 협정에 의해 국가 간 이전이 가능하다.

---

12) White-list에 실린 국가들의 목록은 EU Information Commissioner's Office에서 확인할 수 있다.

13) Directive 95/46/EC Art. 26.(6)

14) 현재 EU 집행위원회는 Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, Switzerland, Eastern Republic of Uruguay, US (EU-US Privacy Shield)가 적절한 수준의 보호를 제공하는 것으로 평가하고 있다. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (검색일 : 2016. 3. 23.)

15) 임규철, 2007, "개인정보의 국외이송에 대한 법적 통제의 필요성 : 한 · 미 FTA의 금융신용정보 국외이송의 문제점을 중심으로", 『인권과 정의』 제365호, 159-175쪽.

3. 유럽사법재판소 판결

(1) 사건개요

EU 지침은 개인정보의 적절한 보호수준(adequate level of protection of the data)을 제공하는 경우에는 제3국으로 개인정보를 이전할 수 있도록 규정하고 있고, EU 집행위원회(EU Commission)는 미국과 개인정보의 국가 간 이전에 관한 세이프 하버 협정을 체결하여 미국 기업들이 EU 회원국 국민의 개인정보를 수집 · 이용할 수 있는 근거를 마련하였다. 그런데 2008년부터 페이스북(Facebook) 이용자였던 오스트리아의 대학생 막스 슈렘스(Maximillian Schrems)의 청원으로 세이프 하버 협정에 대한 문제가 제기되었다. 막스 슈렘스는 페이스북에 제공했던 자신의 개인정보가 페이스북 아일랜드 자회사에서 미국에 있는 서버로 이전되어 처리되었는데, 스노든 사건에서 드러난 사실관계를 바탕으로 보면 미국의 법과 실무 상 미국으로 이전된 정보가 NSA 등 미국의 공적 기관에 의한 감시로부터 충분히 보호받고 있지 못하다고 주장하며 아일랜드 정보보호청에 청원을 제기하였다. 그러나 아일랜드 감독기구는 EU 위원회가 미국 상무부와 적절한 보호 수준 제공을 위한 자발적 체계를 구축하기 위해 2000년 7월 26일 세이프 하버 협정을 체결, 시행하고 있다는 이유로 해당 청원을 거절하였다.[16] 이 세이프 하버 협정에 의해 4,000개 이상의 미국 기업들이 EU로부터 미국으로 개인정보를 이전할 수 있었다. 그런데 2015년 10월 6일 유럽사법재판소는 지난 15년 가까이 유지해 온 세이프 하버 협정을 무효화하는 판결을 선고하였다.[17]

(2) 판결의 주요 내용

유럽사법재판소 판결의 핵심 내용은 세이프 하버 체계가 EU지침 하에서 요구되는 적절한 개인정보보호 수준을 충족시키지 못한다는 것이다. 그 이유는 미국으로 전송되는 EU 회원국 국민의 개인정보에 대한 미국 정보기관의 접근이(특히 세이프 하버 협정에 대한 문언적 검토에 비추어 세이프 하버 협정이 엄격한 관점에서 필수적이고 필요한 범위를 초과하여 미국 집행당국의 개인정보에 대한 접근을 허용한다는 점에서) 유럽 기본권 헌장에 의해 보장되는 사생활의 자유와 권리 및 개인정보보호에 대한 권리를 침해하며, 미국의 감청이나 감시와 관련해 유럽 시민이 질의하는 경우 적절한 회신을 받을 수 없는 상황은 유럽 기본권 헌장에 의해 보호되는 효과적인 침해 제거 및 보상에 대한 유럽 시민의 권리를 침해한다는 것이다.

유럽사법재판소는 EU 집행위원회가 세이프 하버 협정을 채택하였더라도, EU 회원국 내

16) 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council.

17) C-362/14, Maximillian Schrems v Data Protection Commissioner.

의 개인정보보호 감독기구가 제3국으로의 개인정보 이전이 EU지침의 요건을 준수하였는지를 독자적으로 검토할 권한을 가진다고 판단하였다. 궁극적으로는 EU 집행위원회의 결정이 유효한지를 결정할 권한은 유럽사법재판소가 가진다며 유럽사법재판소는 세이프 하버 협정의 무효를 선언하였다.

(3) 판결의 효과

유럽사법재판소 판결에 따라 개인정보보호감독기구가 허가하거나 EU 지침의 예외에 해당하지 않는 이상 세이프 하버 협정에 의한 EU에서 미국으로의 개인정보 이전은 불법이 되었다. 따라서 세이프 하버 협정에 따라 EU 자회사로부터 미국 모회사나 다른 미국 법인으로 개인정보를 이전하던 다국적 기업은 새로운 협정이 체결되기 전까지 구속력 있는 기업 규칙(Binding Corporate Rules: BCRs)과 같이 세이프 하버 협정을 대체할 수 있는 체계를 모색했다. 그러나 이번 판결을 기초로 즉각적인 법집행이 이루어질 것으로 예상되지는 않는다. EU 회원국 내의 정보보호감독기구들은 일정한 유예기간을 허용할 것으로 예상되며, EU 지침에서 요구하는 적절한 보호 수준과 조화하기 위한 노력을 기울일 것으로 예상된다.

한편, 세이프 하버 협정이 무효화되었기 때문에 이를 대체하는 협정의 체결이 불가피해졌고, 미국과 EU는 신속히 협상에 나서 지난 2월초 EU와 미국 간 '프라이버시 보호막(EU-US Privacy Shield)'을 타결했다. 이전에도 EU 개인정보보호규정안의 입법추진 과정에서 세이프 하버 협정의 개정 논의가 진행된 바 있고, 2013. 11. 27. EU 집행위원회가 투명성, 대체적 분

쟁해결 체계의 구제, 집행 개선, 미국 당국에 의한 접근 등 13개 권고를 마련하기도 했다. 그러던 중 이 번 세이프 하버 무효 판결이 나오면서 난항을 겪던 세이프 하버 협정 개정 논의에 속도가 붙게 되었다. 더불어 미국 내에서도 변화의 흐름이 생겨났다. 2014년 1월 오바마 정책 지침 28(Presidential Policy Directive 28)은 정보보호 관점에서 미국 국가안전보장국(NSA)의 업무수행에 일정한 제한을 가하여 EU의 요구를 수용하려는 노력을 보였다. 특히 새로운 협정의 타결에 큰 장애가 되었던 것이 개인정보 침해 시 구제(Redress)가 가능하도록 미국 법률을 제 · 개정하는 것이었는데, 프라이버시 보호막 체결 직후 미국 정보기관의 잘못된 개인정보 사용에 대해 구제받을 권리를 보장하는 사법구제법(Judicial Redress Act)이 미국 의회를 통과함으로써 새로운 협약 체결과 시행을 앞당겼다.

세이프 하버 협정 무효 판결을 둘러싼 일련의 과정은 글로벌 인터넷 경제를 좌우하고 있는 기업들의 요구에 힘입어 개인정보의 자유로운 국가 간 이전을 주장해온 미국과, 개인의 자유와 권리를 강하게 보호하고자 하는 EU의 개인정보보호 정책의 충돌을 상징적으로 보여준다. 그러나 새로운 협약 체결을 통해 개인정보의 활용 못지않게 개인정보의 보호가 중요하다는 점을 양 진영이 공통적으로 인식하기에 이르렀다. 한편, 이 글에서는 자세히 소개하지 못했지만 EU의 개인정보보호규정안이 최종적인 합의에 이르는 과정에서 개인정보에 대한 강력한 보호 요구만큼이나 개인정보의 안전한 활용 요구도 상당 부분 수용되었다는 점을 주목할 필요가 있다. 결과적으로 EU의 개인정보보호규정 최종안에는 개인정보의 합리적인 이용을 가능하게 하는 개인정보처리 기준이 입법화되었다. 즉, 개인정보에 대한 법적 규율은 그 보호와 활용을 조화시키는 합리적인 선상에서 이루어지는 것이 중요하다. 이제 우리도 이러한 차원에서 개인정보보호에 관한 법제를 정비하고 해석 · 적용을 위한 합리적인 기준을 설정, 유지할 필요가 있다.