

[데이터 경제 시대의 도래, 기업이 대비해야 할 주요 법안서]

2차시. 개인정보보호의 국제적 동향

학습목표
<ul style="list-style-type: none">▪ 학습내용: 해당 차시에서 학습할 학습주제(목차)를 제시해 주세요.▪ 학습목표: 해당 차시 학습을 통해 <u>학습자들이 달성해야 할 목표</u>를 학습내용과 연계하여 작성해 주세요.

▶ 학습내용

1. 개인정보보호 법제화의 국제적 동향
2. 개인정보보호의 국제화가 우리나라에 미치는 영향

▶ 학습목표

1. 개인정보보호 법제화의 국제적 동향에 대해 설명할 수 있다.
2. 개인정보보호의 국제화가 우리나라에 미치는 영향에 대해 설명할 수 있다.

학습내용
<ul style="list-style-type: none"> ▪ 학습내용의 위계 파악을 위해 일관성 있는 번호 체계로 작성해 주세요.

I. 개인정보보호 법제화의 국제적 동향

1. 개인정보 보호를 위한 국제화

1) 배경

데이터3법의 가장 기본이 되는 법률은 개인정보보호법이다. 우리나라의 개인정보 보호법은 2011년 3월 29일에 제정되고, 같은 해 9월 30일부터 시행되었다. 그렇다면 개인정보보호 관련 외국의 법제화는 언제부터 시작되었으며, 또한 국제사회에서 개인정보보호는 어떤 표준기준을 마련하고 있을까? 인터넷을 통해 이제 개인정보를 활용한 서비스는 자국민만을 대상으로 하지 않는다. 이미 개인정보를 활용한 글로벌한 다국적 서비스는 어렵지 않게 이용할 수 있다. 인터넷과 결합하여 컴퓨터 뿐만 아니라 이제 핸드폰을 통해 이용되는 수많은 개인정보 활용서비스는 많은 경우 회원가입을 통해 개인정보를 필요로 하고 있다. 이제는 일상이 되어버린 수많은 정보 활용 서비스를 누리기 위해서 개인정보 제공은 거의 필수적 요소가 되었다.

우리나라 기업이나 개인이 개발하는 인터넷서비스를 외국인이 외국에서 이용할 수도 있으며, 외국 기업이나 개인이 개발하는 인터넷서비스 또한 우리나라 국민이 우리나라에서 이용할 수도 있다. 이에 따라 개인정보 보호를 위한 국제적인 표준을 살펴보는 것은 우리나라 기업 및 국민에게 매우 유용할 수 있다.

2) 국제적 노력의 시작

개인정보보호의 필요성은 컴퓨터와 인터넷을 기반으로 하는 ‘지식정보의 혁명’으로 불리는 3차 산업혁명의 도래로 주장되었다. 이러한 3차 산업혁명의 대표적인 특징은 바로 ‘정보의 공유’이고, 공유하는 정보의 범위는 지식정보에 국한하지 않으며, 개인정보까지 확대되기에 이르면서 개인정보 유출에 대한 우려가 전세계적으로 확산되었다. 이에 따라 개인정보 유출은 물론이고 개인정보 오·남용에 대한 폐단을 막기 위해 전세계 각국에서 개인정보보호를 위한 법제화의 요구가 시작되었다.

이로부터 개인정보보호를 위한 법제화는 1970년대부터 유럽 및 미국을 중심으로 하여 논의가 시작되었다. 이러한 논의는 실제로 자국 안에서 행해지는 개인정보를 활용한 각종 자동처리를 규율하여 개인정보를 보호하기 위한 법제도를 확립의 기반이 되었다. 가장 빠르게는 독일에서 추진되었다. 즉 1970년 독일 내 헤센(Hessen)주(州)에서 가장 먼저 개인정보보호법(Datenschutzgesetz)을 제정하면서 시작되었다. 그러나 이러한 헤센주의 개인정보보호법은 독일 전지역이 아닌, 헤센주 차원에서의 개인정보 보호를 위한 법제라는 점에서 큰 역할을 하지는 못하였다.

국가차원의 개인정보보호에 관한 법률은 1973년 스웨덴에서 처음 제정된 것으로 알려져 있다. 이후 1974년 미국에서 공공부문에서의 연방법인 프라이버시법(Privacy Act of 1974)이 제정되었으며, 1977년에는 독일에서, 그리고 1978년에는 프랑스에서 개인정보보호에 관한 법률이 순차적으로 제정되었다.

이처럼 유럽과 미국에서 개인정보보호 관련 법제화가 확대되었으나, 두 지역에서의 관련 법

를 내용은 큰 차이가 있다. 개인정보보호의 대표적인 정책적 방안으로는 정부의 개입이 필연적으로 뒤따를 수 밖에 없는데, 이러한 정부개입을 두고 유럽(EU)과 미국에서의 입장차이가 크다고 할 수 있다. 즉 EU를 중심으로 하는 유럽에서는 개인정보보호에 대하여 상대적으로 보다 강력한 정부개입에 따른 규율을 강조하고 있으나, 반면에 미국에서는 정부개입의 가능성을 보다 축소하고 자율적 규제를 지향하고 있다. 이는 결국 미국에서는 산업서비스의 확대에 초점을 두고 있음을 알 수 있고, 반면에 유럽에서는 개인의 정보권에 보다 더 비중을 두고 있음을 알 수 있다. 이러한 법제화를 간략히 살펴보면 아래와 같다.

2. 국제연합(UN)

개인정보는 개인의 프라이버시와 밀접한 관련을 맺고 있다. 개인정보 안에는 그 개인을 특정할 수 있는 많은 정보들이 축약해 담겨있으므로 자칫 정보가 외부로 공개될 경우에는 개인의 프라이버시침해가 막대하기 때문이다. 이로부터 국제연합인 UN에서는 개인의 프라이버시 보호와 개인정보보호를 위해 여러 다양한 조약과 결의를 마련해두고 있다.

먼저 프라이버시에 대한 보호와 관련해서는 1948년 12월 10일에 개최된 UN총회에서 채택된 세계인권선언(Universal Declaration of Human Rights)을 들 수 있다. 세계인권선언 제 12조에서는 “어느 누구도 자신의 프라이버시, 가족, 주거 또는 통신에 대해 자의적인 간섭을 받지 않으며, 또한 자신의 명예와 명성에 대하여도 공격받지 아니한다. 모든 사람은 그러한 간섭이나 공격으로부터 법의 보호를 받을 권리가 있다.”¹⁾고 선언하고 있다.

Universal Declaration of Human Rights

Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

뿐만 아니라 1966년 12월 16일 개최된 UN총회에서 채택된 ‘시민적 및 정치적 권리에 관한 국제규약(International Covenant on Civil and Political Rights)’²⁾에서도 개인의 사생활 보호를 강조하고 있다. 동 규약 제17조에서는 “1. 어느 누구도 자신의 프라이버시, 가족, 주거 또는 통신에 대하여 자의적이거나 불법적인 간섭을 받거나 그의 명예와 명성에 대한 불법적인 공격을 받아서는 아니된다. 2. 모든 사람은 그러한 간섭 또는 공격으로부터 법의 보호를 받을 권리가 있다.”고 위에서 살펴본 세계인권선언과 유사한 내용을 다시 한번 더 천명하고 있다.

International Covenant on Civil and Political Rights

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference

1) <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

2) <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

or attacks.

보다 직접적으로 개인정보를 보호하기 위한 UN규약은 1990년에서야 비로소 마련되었다. 즉 1990년 12월 14일 개최된 UN총회에서 ‘전산처리된 개인정보파일의 규제를 위한 가이드라인(Guidelines for the regulation of computerized personal data files)’³⁾을 채택하여 회원국에 제시하였다. 동 가이드라인에서는 개인정보파일의 컴퓨터 처리와 관련한 정보주체의 프라이버시권과 인권보장의 기준을 제시하였다는 점에서 개인정보처리와 관련된 보다 직접적인 규정으로 간주되고 있다. 특히 정보주체의 종교, 인종, 성 등의 차이에 따른 차별을 받아서는 안된다는 정보주체의 인권보호를 더욱 강조하였다.

이러한 가이드라인은 컴퓨터를 통한 개인정보의 처리를 위하여 각국의 입법에서 제공되어야 하는 최소한의 보장에 관한 기준으로 다음의 규범원칙을 제시하였다는 데에 큰 의미가 있다. 즉, 공정성의 원칙(Principle (1) of Fairness), 정확성원칙(Principle (2) of Accuracy), 목적 구체화 원칙(Principle (3) of Purpose-specification), 이해당사자 접근 원칙(Principle (4) of interested-person access), 비차별 원칙(Principle (5) of non-discrimination), 예외의 권한 원칙(Principle (6) of the power to make exceptions), 안전원칙(Principle (7) of security) 등의 실질적인 가이드라인을 제시한 것이다.

여기에서 더 나아가 국제연합(UN)은 현재 디지털시대라는 시대적 상황을 직시하여, 정보처리가 폭발적으로 증가할 것을 예측하고 개인정보의 불가피한 사용과 프라이버시침해에 대비하고자 하였다. 이처럼 개인정보와 프라이버시에 대한 보호의 필요성이 증가하여, 2013년 12월 18일 개최한 UN총회에서 ‘디지털시대의 프라이버시에 대한 권리(The Right to privacy in the Digital Age)’⁴⁾에 대한 결의가 채택되었다. 동 결의안은 특히 온라인을 둘러싼 감시에 대한 논란에서 시작되었는데, 당시 미국 국가안보국(NSA)의 대량 불법감시가 폭로되면서 ‘프라이버시권’이 정치적인 문제로 크게 떠오르기 시작하였다. 이로부터 국제연합은 개인정보에 대한 수집 제한을 주요 쟁점으로 하여 동 결의안이 UN총회에 상정되었고, 회원국의 만장일치로 통과되었다. 이러한 결의안은 구속력이 없다는 점에서 비중있게 다루지 않기도 하지만, 동 결의안은 온라인에서의 개인의 프라이버시 보호권을 공개적으로 합의했다는 점에서 주목받았다.

동 결의안이 제시하고 있는 ‘디지털시대의 프라이버시권’ 보호는 크게 다음의 네가지를 기준으로 각 회원국이 이를 준수하도록 촉구하였다.

- I. 디지털 통신 영역을 포함하여 모든 인간의 사생활(프라이버시)를 존중하고 이를 보호할 것
- II. 프라이버시 보호권의 침해를 중단시키고 해당 위반 행위를 막을 수 있도록 각 국의 관련 국내법을 국제인권협약에 맞도록 개정할 것
- III. 국제인권협약에 따라 개인의 프라이버시가 완전하고 효과적으로 보장될 수 있도록 통신활동의 감시, 개인 데이터의 수집 및 탈취 행위와 관련한 절차 및 법 규정의 재검토를 실시
- IV. 국가에 의한 통신활동의 감시, 개인 데이터의 수집 및 탈취행위에 대해 적절하고 책임있는 내부감시 활동을 수행할 투명하고 독립적인 메커니즘 확보할 것

3) <https://digitallibrary.un.org/record/43365>

4) <https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age>

이처럼 동 결의는 프라이버시권을 중심으로 하여, 오프라인에서의 권리로서 뿐만 아니라, 온라인에서도 보호되어야 함을 다시 한번 강조한 것이다. 또한 UN에 가입한 모든 회원국들이 동규약으로부터 디지털통신에서 프라이버시권을 존중하고 보호하도록 요청하였다.

3. 경제협력개발기구(OECD)

경제협력개발기구인 OECD(Organisation for Economic Co-operation and Development)에서도 개인정보 이동에 대한 보호의 가이드라인을 제시하였다. 즉 1980년 9월 23일 개최한 OECD 이사회에서, 국가들간의 개인정보의 자유로운 이동을 보호하기 위해 ‘프라이버시와 개인정보의 초국경 이동의 보호를 규율하는 가이드라인(Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data⁵⁾, 일명 ‘1980년 OECD 프라이버시 가이드라인’⁶⁾을 채택하였다.

동 가이드라인은 OECD 이사회의 권고형식으로 1980년에 채택된 것이어서 위에서 살펴본 UN 결의안처럼 법적 구속력을 갖고 있는 것은 아니다. 하지만 회원국들이 프라이버시 보호를 명목으로 개인정보의 국가간 자유로운 이동을 부당하게 저해하지 않도록, 동 가이드라인의 원칙들을 자국에서 반영하여 협력할 것을 권고하고 있다. 이처럼 동 가이드라인은 비록 강한 구속력을 갖고 있는 것은 아니지만, 그 주된 목적이 각 국가별로 제정 및 논의되고 있는 개별적이고 상이한 프라이버시법을 서로 조화롭게 함으로써 국가간에 정보의 자유로운 이동을 활성화하고 개인정보 처리로 인한 프라이버시 침해를 방지하고자 제정된 것이다. 이처럼 동 가이드라인은 OECD의 특성이 잘 반영된 것인데, 경제적 발전을 목적으로 하는 OECD에서 이러한 개인정보를 보호함으로써 기본적인 프라이버시를 존중하여 개인정보를 경제적 발전에 긍정적으로 활용하기 위함으로 볼 수 있다. 즉 바꿔말하면 한편으로는 개인정보를 보호하고자 하는 목적을 가지고 있는 동시에, 다른 한편으로는 개인정보에 대한 지나친 보호로부터 회원국의 경제발전에 저해하는 것을 방지하기 위한 의미도 갖고 있는 것으로 해석되기도 한다.

동 가이드라인 제2조에서는 가이드라인의 적용범위를 설정하고 있는데, 공공부문과 민간부 무 모두 적용하여, 각 부문에서 처리되는 형태 내지 성질 또는 이용되는 정황을 이유로 개인의 프라이버시와 자유에 대한 위협을 야기하는 개인정보 처리에 적용됨을 밝혔다. 동 가이드라인은 공식명칭 보다는 가이드라인 일부내용인 제7조부터 제14조에서 제시하는 기본원칙에 따라, ‘OECD 프라이버시보호 8대 기본원칙(Basic Principles of National Application)’⁶⁾으로 보다 더 많이 알려져 있는데, 이를 살펴보면 아래와 같다.

No	원칙	조문	내용
1	수집제한 원칙 (Collection Limitation Principle)	7조	개인정보의 수집은 제한되어야 하고, 수집하는 경우 합법적이고 공정한 절차에 따라, 적절한 경우 정보주체에게 알리거나 동의를 받아야 한다. ⁷⁾
2	정보 정확성 원칙 (Data Quality Principle)	8조	개인정보는 그 이용 목적에 부합하는 것만을 수집하여야 하고, 수집목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태를 유지하여야 한다. ⁸⁾

5) <https://www.oecd.org/sti/ieconomy/>

6) <https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflows ofpersonaldata.htm#part3>

3	목적 명확성 원칙 (Purpose Specification Principle)	9조	개인정보 수집 목적은 정보수집 시점에 명시되어야 하고, 그 이후의 이용은 이러한 수집목적 또는 이러한 목적과 모순됨이 없어야 하며, 목적이 변경되는 경우에는 변경시마다 이러한 목적에 명확히 충족하여야 한다. ⁹⁾
4	이용제한의 원칙 (Use Limitation Principle)	10조	개인정보는 수집된 목적으로만 이용하여야 하며, 목적 이외로는 이용해서는 안된다. (다만 정보주체에게 동의를 얻었거나(a) 또는 법에 근거하여 허가된 경우(b)는 예외로 함) ¹⁰⁾
5	안전성 보장의 원칙 (Security Safeguards Principle)	11조	개인정보는 개인정보의 분실, 무단접근, 훼손, 사용, 수정 또는 공개 등과 같은 위험에 대비하여 합리적인 보안조치에 따라 보호되어야 한다. ¹¹⁾
6	공개성의 원칙 (Openness Principle)	12조	개인정보에 관한 개발, 관행 및 정책에 대한 내용이 포함된 공개방침이 있어야 한다. 개인정보처리자(data controller)의 신원과 일상적 거주지와 함께 개인정보의 존재와 특성, 이용의 주된 목적을 쉽게 확인할 수 있도록 하여야 한다. ¹²⁾
7	개인참여의 원칙 (Individual Participation Principle)	13조	정보주체는 개인정보처리자가 자기에 관한 정보를 갖고 있는지 여부에 대하여 개인정보처리자 또는 기타의 자로부터 확인을 받을 권리, 개인에 관한 정보를 상당 기간 내에 과다하지 않은 비용으로 합리적인 방법과 알기 쉬운 형태로 본인에게 통지하도록 하는 권리, 그리고 이상의 요구가 거부당한 경우에는 그 이유를 밝히도록 하고 이와 같은 거부에 대하여 이의를 제기할 수 있는 권리, 자기에 관한 정보에 대하여 이의를 제기하고 그 이의가 인정되지 아니할 경우에는 그 정보를 삭제·개정·보완·수정하게 하는 권리를 갖는다. ¹³⁾
8	책임의 원칙 (Accountability Principle)	14조	개인정보처리자(data controller)는 위에서 제시한 원칙들이 지켜지도록 필요한 제반조치를 취하여야 한다. ¹⁴⁾

7) Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

8) Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

9) Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

10) Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

11) Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

12) Openness Principle

이러한 1980년 OECD 프라이버시 가이드라인은 30여년이 지난 2013에서 개정되었다. 개인 정보가 경제는 물론이고 사회 및 일상생활에서 중요한 역할을 할 뿐만 아니라, 정보 및 통신 분야의 괄목할만한 성장으로 개인정보를 접목한 서비스는 사회적으로, 경제적으로 많은 이익이 될 수 있음을 인지하여 개인정보를 둘러싼 환경변화를 감지하였다.

[표 #: OECD 가이드라인 개정의 배경¹⁵⁾]

<ul style="list-style-type: none"> - 글로벌 서비스가 증가하고, 국가간의 지속적이고 동시다발적인 정보의 흐름 발생 (예: 라인, 페이스북, 트위터 등 글로벌 서비스 등장) - 데이터의 분석을 통해 개인의 움직임, 흥미, 활동 등을 예측하여 잠재적으로 활용할 수 있는 가능성 증가 (예: 빅데이터를 활용한 맞춤형 광고) - 개인의 모든 활동은 어떤 형태로든 디지털 기록으로 남게 되어 그에 따라 감시가 더욱 용이 (예: 스마트폰, 교통카드, 신용카드 등의 사용 증가로 모든 정보를 전자적으로 기록) - 개인정보의 범위가 방대해지고 처리가 빈번해지면서 유출 위험도 함께 증가 (예: 국내에서 2011~12년 해킹으로 유출된 개인정보는 약 6000만 건)

위와 같은 환경의 변화를 감지하여 OECD는 위의 가이드라인을 개정하여 2013년 7월 11일 OECD 이사회에서 '프라이버시 가이드라인에 관한 권고'에서 회원국들이 '프라이버시, 개인적 자유 및 정보의 세계적 자유이동의 기본적 가치를 촉진하고 보호하는데 공동의 이익'이 있음을 인정하였다. 개정된 주요내용은 아래와 같다.

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

13) Individual Participation Principle

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him
 - i) within a reasonable time;
 - ii) at a charge, if any, that is not excessive;
 - iii) in a reasonable manner; and
 - iv) in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

14) Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

15) OECD의 프라이버시 가이드라인 개정(https://blog.naver.com/n_privacy/80205872326)

[표 # : 2013 OECD 프라이버시 가이드라인¹⁶⁾]

<p>(1) 새로운 용어의 정의</p> <p>: 개인정보보호 활동을 지원하고 구체적으로 설명하기 위해 아래와 같은 새로운 용어를 추가적으로 정의함</p> <ul style="list-style-type: none"> - 국가 프라이버시 전략 (National privacy strategies): 정부차원에서 프라이버시와 관련된 정책을 수립하고 조율하여 다차원적인 전략을 수립하는 것을 의미 - 프라이버시 관리 프로그램 (Privacy management programmes): 개인정보를 처리하는 공공기관 또는 기업(이하 ‘개인정보 관리자’라 함)이 개인정보보호 활동을 할 수 있는 절차 등 핵심 운용 메커니즘을 의미 - 데이터 보안 유출 통지 (Data security breach notification): 개인정보의 유출이 발생한 경우 관련 기관과 정보주체에게 이를 알리는 통지하는 것을 의미 <p>(2) ‘개인정보 관리자의 책임 이행’에 관한 내용 신설</p> <p>: 개인정보 관리자가 책임을 준수하기 위한 활동으로 보호활동의 실행방안 수립, 적절한 보호조치 적용, 사고대응을 위한 계획 및 절차의 수립, 지속적인 모니터링 및 감사 등의 ‘프라이버시 관리 프로그램’을 마련하여 이를 시행하고, 이에 따른 활동 기록을 관리하도록 함</p> <p>(3) 개인정보의 국외 이전</p> <p>: 개인정보의 국외 이전에 대해서는 이를 안전하게 보호할 수 있는 최소한의 기준과 관리 책임에 대한 내용을 포함하고 있음</p> <p>즉, 개인정보가 국외로 이전 되었더라도 관리책임은 개인정보 관리자에게 있으며, 국외 이전에 대한 제한은 개인정보의 민감도, 처리에 대한 목적, 이용되는 상황과 존재하는 위험을 고려하여 판단하도록 안내함</p> <p>(4) 국내이행을 위한 ‘프라이버시 집행기관’ 설립</p> <p>: 국가가 개인정보보호를 위한 활동을 효율적으로 할 수 있도록 거버넌스, 자원, 기술적 전문지식을 가지고, 객관적으로 공정하게 일관된 기준으로 의사결정을 할 수 있는 ‘프라이버시 집행기관’의 설립에 관한 내용을 포함함</p>
--

한편 이러한 OECD의 가이드라인에 따라 회원국의 하나인 우리나라도 이러한 가이드라인을 준수하여야 하는데, (4)에서의 요청에 따라 우리나라에서 ‘프라이버시 집행기관’으로는 안전행정부, 방송통신위원회, 개인정보보호위원회 등이 대표되고 있다.

4. 유럽연합(EU)

유럽연합(EU)도 1994년 10월 24일 ‘개인정보의 보호 및 자유로운 이전에 관한 유럽의회와

16) OECD의 프라이버시 가이드라인 개정(https://blog.naver.com/n_privacy/80205872326)

이사회 지침(축약하여 'EU의 개인정보보호지침' 또는 '95/46/EC'로 불림)¹⁷⁾을 마련하였다. 동 지침은 EU회원국 시민들의 기본권과 자유, 특히 개인정보 처리에 있어서 프라이버시를 보호하기 위한 일반적인 개인정보보호지침이다. 이러한 EU의 개인정보보호지침은 기본권과 연결되고 있는데, 기본권에 관한 별도의 법적 문서로 EU기본권헌장이 채택되어, 이러한 기본권이 바로 EU의 핵심적인 법적 기반이 된다고 한다. 특히 독일과 프랑스 등에서 보다 엄격한 수준의 개인정보보호를 주도하였고, 이로부터 EU의 개인정보보호 정책 등이 개인정보보호의 국제기준으로 자리잡게 되었다고 한다.

1995년 10월 24일 EU 개인정보보호지침이 채택되기 이전에도 EU회원국에서는 각국 나름의 개별적인 개인정보보호를 위한 법체계를 갖추고 있었다. 그러나 각 회원국의 문화, 전통, 사회적 환경 등에 따라 개인정보에 대한 보호수준이나 기준이 상이하였다. 따라서 개인정보 처리가 국제적으로 이용되는 상황을 고려하여 이들 각국의 기준을 조화롭게 할 필요성이 요구됨에 따라 EU 개인정보보호지침이 마련되었다.

1) EU 개인정보보호지침

이처럼 EU 개인정보보호지침은 EU 회원국 시민들의 개인정보가 회원국 어디서나 동일한 수준으로 보호될 것을 보장함을 목표로 하였다. 동 지침은 총 7장 34조로 구성되었다. 동 지침 제1조에서는 제정목적을 내용으로 하고 있다. 즉, '1. 동 지침에 따라 회원국들은 자연인(natural person)의 기본적 권리와 자유, 특히 개인정보 처리에 관하여 프라이버시에 대한 권리를 보호하여야 한다. 2. 회원국들은 위 제1항에 근거하여 주어지는 보호와 관련된 이유를 들어 회원국들 사이의 개인정보의 자유로운 이동을 제한하거나 금지해서는 아니된다'라고 규정하였다.

보다 구체적으로는 EU 회원국 내에서 첫째, 개인정보 처리에 관한 의무와 책임을 확립하고, 둘째, 개인정보 처리의 투명성이 유지되도록 보장하며, 셋째, 민감한 정보에 대한 특별한 보호기준을 설정하고, 마지막으로 넷째, 개인정보 처리에 대한 효과적인 감독권과 집행권을 확보하는 것이 그 목표라고 설정하고 있다.

이러한 EU 지침은 유럽연합 의회와 이사회에 의하여 채택된 지침이다. 따라서 EU회원국들은 동 지침의 이행을 위하여 새롭게 개인정보보호법을 제정하거나 기존의 법률을 개정하여야 했다. 동 지침은 OECD 가이드라인과는 달리, 기본적으로 자동화된 수단에 의한 개인정보의 처리에 적용된다. 물론 전적으로 자동화된 수단에 의한 정보처리만을 의미하는 것은 아니다. 즉, 일부 자동화된 수단에 의한 경우에도 적용될 수 있고, 뿐만 아니라 자동화된 수단이 아닌 다른 방법에 의해 처리된다 하더라도 개인정보가 파일링시스템(filing system)¹⁸⁾의 일부를 구성하거나 그러한 의도로 처리되는 경우에도 동 지침은 적용된다. 즉, EU 지침은 모든 개인정보의 자동화된 처리 및 '구조화된 수기파일(structured manual files)'에 적용되는 것으로 볼 수 있다.

나아가 동 지침은 자연인(natural person)에 대한 개인정보보호를 위한 것이며, 법인(legal

17) DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

18) 파일링시스템(filing system)에 대해서는 EU 지침 제2조에 규정하고 있다. 즉 기능적으로 또는 지리적적으로 집중·분산·산재되어 있는지 여부와는 관계없이, 특정한 기준에 따라 접근할 수 있는 모든 개인정보의 구조화된 장치를 의미한다.

person)에 대한 정보를 보호대상으로 삼는 것은 아니다. 하지만, EU 회원국이 법인의 정보를 보호하는 내용을 규정에 두는 것까지 규제하는 것은 아니어서 법인에 대한 정보보호는 회원국 각국에서 국내법으로 마련하면 된다.

2) EU 개인정보보호지침과 OECD 가이드라인의 차별점

이러한 EU의 지침은 또한 개인정보 처리에 관한 프라이버시에 대한 권리를 포함하여 개인의 기본권과 자유에 대한 보호를 목적으로 함으로써 회원국들 사이에서 개인정보의 자유로운 이동이 제한받지 않도록 하는데 있다. 즉 개인정보에 대한 보호를 주목적으로 하면서도 동시에 회원국간에 개인정보를 자유롭게 활용하도록 한 것이다. 이에 따라 EU의 동 지침은 적용 범위를 제외하고는 앞서 살펴보았던 OECD 가이드라인의 개인정보보호 8원칙을 대부분 수용하는 것으로 평가되고 있다. 다만 차이가 있다면 EU 개인정보보호지침이 원칙적으로 민감한 개인정보의 수집을 금하고 있어서, OECD 가이드라인에 비하여 민감한 개인정보에 대해서는 매우 강력한 개인정보보호의 입장을 피력한다는 점이다. 즉, EU 개인정보보호지침과 OECD 가이드라인 모두 개인정보보호와 개인정보활용을 동시에 목적으로 하고는 있지만, EU 개인정보보호지침은 민감 개인정보를 엄격히 보호함으로써 개인정보보호에 비중을 두고 있는 반면에, OECD 가이드라인은 경제협력개발기구인 만큼 개인정보활용에 좀 더 비중을 두고 있는 것으로 이해될 수 있다.

이러한 차이점은 수집된 개인정보를 제3자에게 제공하거나 공개하는 데에 있어서도 EU 지침과 OECD 가이드라인이 차이를 둔다. 즉 EU 개인정보보호지침에서는 개인정보보호에 보다 더 무게를 둬서 따라 개인정보의 제3자 제공 및 공개하는 경우에 대하여 세부적인 규정을 마련해 두어, 정보주체에게 수집 및 이용목적에 고지함에 있어서 수집된 개인정보를 제3자에게 제공할 수 있음도 함께 고지하도록 하고 있다.

나아가 가장 큰 차이는 독립적인 개인정보보호기구의 역할에 대한 부분이다. EU 개인정보보호지침에서는 독립적인 개인정보보호기구의 설립을 통해서 개인정보의 관리·감독 및 개인정보가 제3국으로 이전하는데 대해 엄격히 제한을 가하고 있다. 즉 EU의 동 지침은 개인정보처리자로 하여금 개인정보 처리행위에 대하여 회원국 내의 독립적인 개인정보보호기구에 그 사실을 사전에 고지토록 하여, 고지받은 개인정보 처리행위가 정보주체의 권리와 자유에 위협이 될 수 있는지 여부를 회원국의 개인정보보호기구가 사전에 심사하여 엄격히 통제할 수 있도록 하고자 하였다.

3) EU 지침의 효력과 ‘프라이버시 라운드’ 등장

EU 지침이 EU 회원국에서 효력을 갖기 위해서는 해당 회원국의 국내법에서 EU 지침을 준수하는 내용이 뒷받침되어야 한다. 즉 회원국은 자국의 개인정보 관련 법률에서 해당 EU 지침의 목적과 내용을 벗어나는 내용을 규정해서는 안된다. 물론 회원국마다 문화, 사회, 환경 등이 다양할 수 있으므로 세부적인 내용은 회원국마다 정보보호에 있어 수준차이가 있을 수밖에 없다. 그럼에도 실제로 28개 회원국에서는 이러한 EU 개인정보보호지침에 따라 일반적으로 동일한 내용으로 이행되고 있다고 한다.

또한 EU 개인정보보호지침은 EU 회원국 외의 제3국이 동 지침에서 밝히고 있는 적절한 수준의 개인정보보호 체계를 갖추고 있지 아니한 경우에는 개인정보를 해당 국가로 이전하지 못하도록 규정하고 있다(제25조). 이 규정은 일명 ‘프라이버시 라운드(Privacy Round)’라 하여,

사실상 새로운 무역장벽으로 인식되고 있다. ‘프라이버시 라운드’란 자국민의 개인정보보호를 위해 세계 각국들이 벌이는 다자간 협상전쟁의 서막을 의미하는 떠오르는 용어이다.

개인정보가 경제적 자산으로 떠오르고 개인정보 유출시 프라이버시 침해가 극심함에 따라 세계 각국에서는 해외로 유출되는 자국민의 개인정보를 보호하기 위한 다방면의 노력을 기울이고 있다. 특히 유럽연합(EU)에서는 미국(의 글로벌 시장)이 주도하는 세계 디지털 시장에서의 주도권을 확보하기 위해 주력하였다. 이에 따라 유럽연합에서는 EU 회원국에 공통적으로 적용되는 개인정보보호규칙인 GDPR(General Data Protection Regulation)을 2016년에 채택하였고, 2018년 5월 25일부터 EU회원국 국민의 개인정보를 다루는 전 세계 모든 기업들에게 적용하는 ‘프라이버시 라운드’, 즉 개인정보를 둘러싼 국가간의 전쟁이 시작된 것으로 평가된다.

4) 유럽의 개인정보보호규칙(GDPR)

가. 도입배경

EU 개인정보보호지침이 회원국들에게 개인정보 관련한 자국의 국내법 제정에 있어서 가이드라인이 되어 통일된 법제마련의 기틀이 되었다는 점에서 중요한 역할을 하였으나, 이후 인터넷을 통한 개인정보 활용의 기술적 발전이 빠르게 진행되면서 이를 반영한 개정된 규제가 필요하다는 인식을 하게 되었다. 즉 미국을 중심으로 디지털시장이 급변하면서 유럽도 이에 대한 대비책이 필요하다는 인식이 강하게 반영된 것이다. 이에 따라 유럽위원회는 2012년 1월 디지털시대의 ‘EU 개인정보보호 개혁(EU Data Protection Reform)’을 제시하였고, 마침내 2016년 5월에 일반개인정보보호규칙(General Data Protection Regulation)이 제정되었다. 이후 2년간 유예기간을 두어 회원국들과 개인정보처리자 등이 GDPR의 적용에 따른 준비기간을 갖도록 하였다. 그리고 2018년 5월 25일에 시행되었다. GDPR은 디지털시대에 걸맞도록 EU 회원국의 기본권을 강화하는 동시에 디지털시장에서 기업을 위해 개인정보보호 관련 법제도를 단순화하여 디지털 관련 사업을 확장하고자 하는 목적으로 제정되었다.

나. 전체 구성 및 효력

GDPR은 서문 173항, 총 11항 99조로 이루어져 있다. 동 규칙이 시행되면서 기존 ‘1995 EU 개인정보보호지침(Data Protection Directive 95/46/EC)은 폐지되게 되었다. EU 개인정보보호지침에 비하여 조문수가 상당히 많이 증가한 GDPR은 이제 개인정보보호와 그 활용에 대하여 매우 구체적으로 적시하고 있음을 알 수 있다. 이러한 GDPR은 앞서 가이드라인이 되었던 EU 지침과 달리 EU 회원국들에게 규칙으로서의 강한 구속력을 가지고 있어서 EU 회원국 모두에게 직접적으로 적용이 되어, 기존 EU 개인정보보호지침에 따른 회원국들 사이에서 보였던 일부 불일치되던 부분이 해소될 것으로 기대를 모았다.

다. 적용범위

GDPR이 일반 개인정보보호 규칙으로서 회원국들에게 강한 구속력을 갖게 됨에 따라 미국은 물론이고 유럽에 마케팅하려는 글로벌업체에게는 주의해야 할 규칙이다. 따라서 유럽에 진출하려는 디지털 관련 사업자는 이러한 GDPR의 적용대상을 인지하고 있어야 한다. GDPR은 EU에 거주하는 자연인인 시민의 개인정보를 처리하는 모든 개인정보 처리자, 정보보호책임자

(DPO) 등이다. 이때 EU 국가에 사업장을 보유하고 있거나, 또는 EU에 사업장을 보유하지 않더라도 EU에 거주하는 정보주체에게 재화 또는 서비스를 제공하거나 정보주체의 행동을 모니터링하는 기업들도 GDPR의 적용대상이 된다. 즉 GDPR에 따라 이제 유럽연합(EU)의 시민에 대한 정보를 활용하는 경우 EU의 회원국이 아니더라도 EU 시민의 정보와 관련한 정보통제자(data controller), 정보처리자(data processor), 정보보호책임자들(data protection officer: DPO)은 GDPR을 준수하여야 한다. 이처럼 GDPR은 EU 시민의 개인정보를 다루는 모든 기업 및 단체가 이들 EU 시민의 프라이버시 보호와 관련된 광범위한 규정들을 준수하도록 강제하고 있는 것이다.

또한 GDPR도 EU 개인정보보호지침과 마찬가지로 개인정보 보호에 대한 EU 시민의 권리를 강하게 보호하는 것을 주목적으로 하면서도 동시에 개인정보 활용을 높이기 위하여 개인정보의 EU내 자유로운 이동이 제한되거나 금지되는 것을 하지 말도록 규정하고 있다(GDPR 제1조 제3항). 이처럼 GDPR에서도 개인정보보호와 개인정보활용이 동시에 충족되도록 요청되고 있는 것이다.

라. 주요내용

GDPR은 정보주체를 위한 개선된 내용을 담고 있을 뿐만 아니라, 정보처리자들(컨트롤러 및 프로세서)을 위한 개선된 의무규정을 내용으로 하고 있다.

먼저 정보주체의 보호를 위한 개선된 내용은 기존의 EU 개인정보보호지침에서의 보호 보다 강력한 보호체계를 갖추고 있다. 즉 정보주체에게 ‘잊혀질 권리(right to be forgotten; 제17조)’, ‘접근할 권리(right of access; 제15조)’, ‘개인정보를 이동할 권리(right to data portability; 제20조)’, ‘개인정보침해시 통지받을 권리(right to be notified of data breaches; 제19조)’, ‘개인정보를 수정할 권리(right to rectification; 제16조)’, ‘개인정보 처리를 제한할 권리(right to restriction of processing; 제18조)’, ‘개인정보 처리에 대한 이의 제기권(right to object; 제14조)’, ‘자동처리의 대상이 되지 않을 권리(rights related to automated decision making including profiling; 제22조)’ 등 다양한 권리를 GDPR 제12~23조에서 명시하고 있다. 이러한 정보주체의 권리는 개인 데이터를 합법적으로 처리하는 기업 및 단체들의 처리를 제한하고 있는 것이다.

그리고 이러한 GDPR을 준수하지 않을 경우, 위반한 기업 및 단체 등에게는 세계적인 연매출의 4% 이하 또는 2천만 유로 이하 중 높은 금액에 대해 과징금을 부과할 수 있도록 강력한 제재장치를 만들었다. 실제로 EU에서는 세계 최대 전자상거래업체인 아마존에게 유럽 시민에 대한 개인정보보호규칙(GDPR)을 위반했다는 이유로 7억4600만유로(약 1조202억원)의 과징금을 부과하기도 하였다. 또한 2019년에는 구글에 5000만유로(약 684억원)에 해당하는 과징금을 부과하였다.

나아가 EU 시민의 정보를 활용하는 기업 및 단체 등은 GDPR 정책을 채택해 시행해야 할 뿐만 아니라, 개인정보 처리활동을 기록해야 하고, 리스크가 있는 처리를 하기 전에 영향평가를 실시하여야 한다. 또한 정보보호 최고책임자(DPO)를 지정하여 EU 시민의 개인정보를 처리함에 있어 책임감 있는 자세를 요구하고 있다. 그리고 기업 및 단체 등이 EU 시민의 개인정보를 침해했음을 인지한 경우에는 그 사실을 알게 된 후 72시간 내에 감독기구에게 뿐만 아니라 침해된 정보주체에게 지체없이 침해사실을 통보하도록 하고 있다.

II. 개인정보보호의 국제화가 우리나라에 미치는 영향

위에서 살펴본 다양한 국제기구의 개인정보보호 법제화는 우리나라에도 많은 영향을 준다. 실제로 우리나라도 국제기구에 가입되어 있는 국제연합(UN), 경제협력개발기구(OECD)의 경우에는 이들 국제기구의 개인정보보호 기준들을 우리도 준수하여야 한다. 이에 발맞춰 우리나라도 개인정보보호법에 각 기구의 가이드라인을 반영하여 개정하고 있다.

또한 EU 회원국이 아니라 하더라도 유럽연합(EU)은 우리 기업의 중요한 시장이다. 따라서 우리나라 기업이나 단체 등이 유럽연합의 시민들을 대상으로 디지털 관련 산업으로 진출할 경우 EU의 최근 정보보호 관련 규정인 GDPR을 준수하여야 하므로 GDPR에 대한 세밀한 분석을 통해 우리나라 기업 및 단체가 피해를 받지 않도록 하여야 한다.

이제 개인정보는 민간부문에서 뿐만 아니라 공공부문에서도 많은 활용을 하고 있다. 나아가 기업이나 단체 뿐만 아니라 개인 또한 어플리케이션 등을 개발함으로써 글로벌시장에 뛰어드는 시대가 도래하였다. 이처럼 오늘날 업무적인 요소로서 뿐만 아니라 일상생활 깊숙이 개인정보를 활용한 서비스가 자리잡고 있으므로 기업이나 정부는 물론이고 개인정보를 활용한 서비스를 개발하여 제공하고자 하는 개인도 국제적인 표준을 눈여겨봄으로써 준수해야 할 내용이 무엇인지 숙지하여야 할 것이다.