Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.3, Jun. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.3.591

무조건적 자기정보접근권 부여에 대한 국내외 규제현황 및 사례분석을 통한 개선방안 연구

배 진 호†‡
고려대학교

A Study on the Improvement of the Unconditional Right to Informational Self-Access Based on the Status of Domestic and Foreign Legislation and It's Application to Domestic Corporations

Jin-ho Bae†‡
Korea University

요 약

개인정보자기결정권이란 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리"로서 2005년 헌법재판소에서 헌법상으로 인정한 권리이다. 개인정보 자기결정권 중에는 정보주체가 정보보유자가 보유중인 본인의 정보에 대한 현황 및 처리내역을 열람할 수 있도록 하는 자기정보접근권이 있다. 이러한 자기정보접근권을 보장하기 위하여 개인정보와 관련된 각종 법률에서 정보보유자에게 개인정보의 처리에 관한 사항을 정보주체에게 무조건적으로 통지하도록 의무(이하 "무조건적 자기정보접근권")를 부여하고 있다. 본 논문에서는 이러한 무조건적 자기정보접근권 부여에 대한 국내 법률 현황 및 외국의 규제 현황을 분석한다. 이어서 국내 기업들의 대응 사례를 소개하고, 관련 문제점 및 개선방안을 제시하며 결론을 낼 것이다.

ABSTRACT

The right to informational self-determination refers to the constitutional right for an individual, which is approved by the constitutional court, to decide what contents the collected information comprises and to control the circulation of information relation to oneself. It contains claim for inspection of personal information(The right to informational self-access) as a right for individual to review information of current state and processing history which information holders have. To assure the right to informational self-access, individual must be notified of the processing history of information by information holders regardless of individual's request(The unconditional right to informational self-access).

This study will analyse current status of domestic and foreign legislation and global regulation which are related to the unconditional right to informational self-access. In addition, the action of domestic corporations will be introduced. Finally, it will be concluded with relevant problems and solutions to solve the problems.

Keywords : The right to informational self-determination, The right to informational self-access

I. 서 론

1.1 무조건적 자기정보접근권 개요

"개인정보자기결정권"은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또† 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다[1].

Received(01. 26. 2017), Modified(04. 12. 2017), Accepted(05. 01. 2017)

† 주저자, jinho.bae@kbfg.com
‡ 교신저자, jinho.bae@kbfg.com(Corresponding author)

현대에서는 정보통신기술의 발달에 따라 개인정보의 데이터베이스 구축 및 처리와 이용이 간편하고 신속하게 이루어질 수 있게 되었고, 네트워크를 통한 여러 기관간의 개인정보의 전송 및 결합도 쉬워졌다.

이러한 변화에 따라 오늘날 개인의 신상이나 비밀에 대한 여러 가지 정보가 본인의 의사와는 전혀 관계없이 정보를 습득한 정보보유자로부터 지속적으로 이용, 확산될 수 있는 환경에 이르렀으며, 이와 같은 상황 하에서 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술 발달에 따른 개인정보의 무분별한 오남용 및 확대의 위험성에서 보호함으로써, 궁극적으로는 개인의 자유를 보호하고, 나아가 자유민주체제의 근간이 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장 장치라고 할 수 있다[2].

개인정보의 수집·이용·제공이 정보주체인 개인의 의사가 무시된 채 이루어지는 경우 개인정보자기결정권을 침해하게 된다. 그러나 이러한 개인의 권리가 절대적인 것은 아니므로 개인정보에 대한 수집·이용·제공에 대해 정보주체가 어느 정도 관여할 수 있을 것인지는 수집목적·이용형태·처리방식 등에 따른 위험성의 정도에 따라 다를 수 있을 것이다. 적어도 정보주체의 인격적 요소인 개인정보가 국가나 사인에 의해 자의적으로 조작·처리되어서는 안 된다는 것이 헌법상 개인정보자기결정권의 기본정신이다[3].

이에 따라 국가나 사인에 의한 개인정보자기결정권의 침해를 예방하고, 침해시 실효성 있는 구제를 위해 익명권, 수집제한청구권, 정보처리금지청구권, 정보열람청구권, 정보정정청구권, 정보차단청구권, 정보분리청구권, 정보삭제청구권 등의 구체적인 권리가 요구된다[4].

이 중 자기정보접근권은 타인에 의하여 처리되고 있는 개인정보의 내용에 대하여 정보주체가 자신에 관한 정보의 열람을 청구할 수 있는 권리를 말하는데, 정보주체가 자신에 관한 정보에 대한 열람을 청구할 경우, 정보보유기관은 정당한 이유가 없는 한 열람을 허용해야 한다는 것이다[5]. 이를 위하여 개인정보보호 관련 법률에서는 정보주체에게 정보보유자가 보유한 본인의 정보현황 및 처리내역에 대한 열람을 요청할 수 있는 권리를 부여하고, 정보보유자는 이러한 요청에 따를 의무를 부과하고 있다.

이러한 방식이 정보주체가 본인의 정보처리 내역에 대한 열람을 요청한 경우에만 발생하는 조건적 권리(이하 "조건적 자기정보접근권")라면 이러한 정보주체의 의사와 무관하게 부여되는 자기정보접근권을 "무조건적 자기정보접근권"이라 한다.

1.2 연구의 필요성

국내 개인정보보호 관련 법률은 종류가 다양하여 정보보유자들은 어떤 법률이 적용되는지 알기 어려워 오히려 개인정보 보호를 저해하는 측면이 존재하였다. 이에 최근에는 이를 해소하기 위해 개인정보보호 관련 법률간 규제의 차이가 좁아지고 내용이 단일화되고 있는 추세에 있다[6].

동시에 개인정보자기결정권 중 자기정보접근권은 최근 개인정보보호 관련 법률에서 정보보유자의 의무로서 두드러지게 강화되고 있는데, 기존에는 조건적 자기정보접근권을 주로 규율하였으나, 최근에는 무조건적 자기정보접근권 방식의 규제가 확산되고 있다.

이에 따라 현재 강화되고 있는 무조건적 자기정보접근권의 효과에 대한 검토가 이루어지지 않는다면, 일부 법령에서 나타난 무조건적 자기정보접근권 방식의 규제가 더욱 확산될 수 있다.

이에 본 논문에서는 자기정보접근권 중 무조건적 자기정보접근권에 대한 효과 및 타당성에 대해 다음과 같은 방식으로 검증해 보고자 한다.

첫 번째로, 무조건적 자기정보접근권이 세계적으로 유사하게 규제되고 있는지 여부를 확인하기 위해 국내외의 자기정보접근권의 현황을 알아본다. 국내의 무조건적 자기정보접근권 방식의 규제가 세계적 규제 현황과 차이가 크다면, 최근 세계경제의 글로벌화와 더불어 클라우드나 빅데이터 등 현재 대두되는 IT기술산업 발전에 필요한 개인정보의 국경간 자유로운 흐름이라는 추세에 역행하게 될 수 있기 때문에 해당 규제방식의 타당성이 떨어진다고 볼 수 있다.

개별 국가 외에 OECD, EU APEC 등 국제기구도 개인정보의 국경간 이전에 관하여 일정한 제한을 두고는 있으나, 기본적인 입장은 개별 국가의 개인정보 법제간의 차이 때문에 개인정보의 국경 간 또는 역내의 자유로운 흐름이 저해되어서는 아니된다고 선언하고 있기 때문이다[7].

두 번째로 국내 대형 금융기관의 무조건적 자기정보접근권 이행 사례를 통해 무조건적 자기정보접근권이 실제 어떠한 방식으로 이행되는지를 알아본다. 또한 해당 권리보장에 따른 자기정보에 관한 내용이 정보주체에게 어느 수준으로 접근되며, 정보주체들은 이에 대해 어떻게 반응하는지를 실제 금융기관에 제

시한 피드백 사례를 통해 알아본다.

이러한 실제 적용 사례 분석을 통해 무조건적 자기정보접근권의 효과를 파악하고, 관련 문제점을 도출한다.

마지막으로 도출된 문제점에 기반하여 무조건적 자기정보접근권 방식 규제의 개선방향을 제시하고 결론을 낼 것이다.

II. 자기정보접근권 보장을 위한 국내 법률 현황

2.1 개인정보보호법

개인정보보호법은 개인정보보호와 관련된 일반법으로써, 타 법률에 개인정보처리와 관련하여 특별히 예외적으로 적용될 수 있는 경우를 제외하면, 모든 정보주체와 정보보유자에게 적용되는 권리 및 의무사항을 규정하고 있다.

개인정보보호법에서의 자기정보접근권은 제20조, 26조, 34조, 35조(개인정보의 열람)에서 규율하고 있다. 개인정보보호법 제20조 제1항, 제35조 제1항, 제3항은 정보주체의 요청에 따라 발생하는, 개인정보보호법 제정 시점부터 유지되어온 조건적 자기정보접근권과 관련된 조항이다.

제20조 제2항 및 제26조는 정보주체의 요청과 무관하게 정보보유자에게 통지의무를 부과한 무조건적 자기정보접근권 보장에 관한 조항이다.

제20조 제2항은 2016년 9월 최초 시행된 사항으로, 제20조 제1항에서 규정하고 있는 정보주체의 요구가 있는 경우의 수집출처, 처리목적, 처리정지요구권의 존재가 있음을 고지하는 조건적 자기정보접근권에 더하여, 처리하는 개인정보의 종류·규모·종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 일정한 규모의 정보보유자는 정보주체의 요청사실여부와 관계없이 반드시 수집출처, 처리목적, 처리정지요구권의 존재를 정보주체에게 고지하도록 하고 있다. 여기서 대통령령으로 정하는 기준에 해당하는 일정한 규모 이상이란 5만명 이상의 민감정보 또는 고유식별정보를 처리하는 자 또는 100만명 이상의 개인정보를 처리하는 자에 해당되며, 통지 시에는 서면·전화·문자전송·전자우편 등의 방법으로 하도록 하고 있다.

제26조 제3항에서는 정보보유자가 서비스 홍보 및 판매 권유하는 업무를 위탁 시에는 서면, 전자우편, 팩스, 전화, 문자전송 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 통지하도록 하고 있다. 다만, 시행령 제28조 제5항에 따라 위탁자가 과실 없이 정보주체에게 알릴 수 없는 경우에는 인터넷 홈페이지 게시 또는 사업장등의 보기 쉬운 장소에 게시하는 것으로 이를 갈음할 수 있도록 하고 있다.

제34조에서는 개인정보가 유출된 경우, 정보보유자가 유출된 개인정보의 항목, 시점과 경위 등을 정보주체에게 통지하도록 의무를 부과하고 있다. 개인정보 유출은 정보주체에게 직접적인 피해를 미칠 수 있는 가능성이 높은 중대한 사고로, 사고발생 시 정보주체의 자기정보접근권을 보장하기 위하여 개인정보보호법이 제정된 시점부터 보장되어온 내용이다.

2.2 신용정보의 이용 및 보호에 관한 법률

신용정보의 이용 및 보호에 관한 법률(이하 “신용정보법”)은 건국 이래 신용정보의 보호를 위하여 제정되었던 단편적 법률과 신용정보의 이용에 관하여 제정된 금융기관 협약 및 관련 정부지침을 집대성한, 국내 신용정보의 유통과 관리에 관한 체계를 관장하는 일반법이다[8].

신용정보법에서의 자기정보접근권은 제20조의2, 35조, 38조, 38조의 2, 39조의2에서 규율되고 있다.

신용정보법 제35조, 38조, 38조의2는 정보주체가 본인정보에 대한 열람을 정보보유자에게 요청 시에 발생하는 조건적 자기정보접근권에 대해 규정하고 있다. 이는 개인정보보호법 제35조에서 규율하고 있는 조건적 자기정보접근권과 본질적으로 동일하지만, 신용정보법 제35조에서는 정보보유자(법상 “신용정보회사등”)가 정보처리내역의 조회를 할 수 있는 시스템을 구축하도록 하여 정보주체의 조건적 자기정보접근권 이행에 대한 편의를 제공하도록 하고 있다.

이는 2015년 3월 공포되어 2016년 3월부터 시행된 사항으로, 2014년 카드사의 고객정보유출사고 등이 발생함에 따라, 신용정보의 보호에 대한 강화 필요성이 제기되어 신용정보유출에 대한 사전적 예방을 강화하고자 하는 취지에 따라 신설된 조항 중 하나이다[9]. 본 조항 신설은 조건적 자기정보접근권의 규율에 있어 기존 정보주체의 권리 및 정보주체의 요청을 따로도록 정보보유자의 의무를 부여하는 수준에서, 조회시스템 구축을 통한 정보주체의 권리 이행 방식의 편의을 보장하도록 하는 방식으로 적극적으로 강화한 데 그 의미가 있다. 이와 유사하게 금융지주회사법에서도 2015년 12월 그룹사간 고객정보 제공

내역에 대한 조회시스템 구축을 의무화하는 조항이 신설되는 등, 조건적 자기정보접근권에 대해서도 정보주체의 권리가 더욱 강화되는 방향으로 법 개정이 이루어지고 있다.

신용정보법 제20조의2, 39조의 2에서는 상거래관계가 종료된 정보주체의 개인정보를 활용하는 경우와 개인정보가 유출된 경우에 대해 정보주체의 요청이 없더라도 정보보유자의 통지 의무를 부여한 무조건적 자기정보접근권에 대한 조항이다. 제20조의2는 2016년 신설된 조항으로, 상거래관계 종료 후 5년이 도과하여 상거래관계에 따라 수집한 개인정보를 원칙적으로 파기해야 함에도, 부득이한 사유로 인해 분리 보관하고 있는 정보를 활용 시에 정보주체에게 그 내역을 통지하도록 의무를 부여하고 있다. 이는 정보주체가 상거래종료에 따라 정보보유자의 본인정보의 처리에 대한 관심이 소홀해 질 수 있는 상황에, 정보보유자의 통지의무를 부과함으로써 정보주체의 인식 불가능한 자기정보접근권을 보장하고자 하는 취지로 판단된다. 이는 정보통신망법에서도 유사하게 시행되고 있는데, 정보주체가 인식하지 못할 개연성이 높은 개인정보처리내역에 대해서는 무조건적 자기정보접근권을 부여하여, 정보주체의 본인정보처리 인지에 대한 사각영역을 제거하고자 하는 취지로 판단된다.

제39조의2는 개인정보보호법 제34조와 동일하게 개인정보가 유출된 경우의 정보보유자의 통지 의무를 규율하고 있다.

2.3 정보통신망 이용촉진 및 정보보호 등에 관한 법률

전산망 보급확장과 이용촉진에 관한 법률(이하 "전산망법")은 전기통신과 전자계산조직의 균형적인 발전 및 효율적인 이용을 촉진하여 정보화사회의 기반조성과 고도화에 필요한 사항을 규정함으로써 정보화사회의 물결을 능동적으로 수용하고 국민생활의 향상과 공공복리의 증진에 기여하고자 1986년 5월 제정되었다[10]. 전산망법의 운영상 드러난 개인정보보호 등 제도상의 문제점을 개선하기 위하여 2001년 1월, 정보통신서비스제공자에 대한 개인정보보호 규제를 강화하는 등 내용을 반영하여 전산망법을 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법")로 개정하였다[11].

정보통신망법상 자기정보접근권 보장은 제27조의3, 30조, 30조의2에서 규율하고 있다. 정보주체의 요청에 따른 조건적 자기정보접근권 보장은 제30조에서 규율하고 있으며, 이는 개인정보보호법 및 신용정보법상의 조건적 자기정보접근권과 본질적으로 동일하다.

무조건적 자기정보접근권은 제27조의3, 30조의2에서 규율하고 있다.

제27조의3은 개인정보유출시의 정보보유자의 통지의무를 규율하고 있는데, 개인정보보호법 및 신용정보법상에서 규율하고 있는 개인정보유출시의 통지의무와 유사하다.

제30조의2에서는 개인정보보호법 및 신용정보법과 비교하여 보다 강화된 무조건적 자기정보접근권을 부여하고 있는데, 100만명 이상의 개인정보를 보유하거나 전년도 매출액이 100억 이상인 정보통신 서비스 사업자는 매년1회 이상 정보주체의 동의에 따라 수집한 개인정보의 이용내역을 전자우편, 서면, 모사전송, 전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 정보주체에게 통지하도록 하고 있다. 제30조의2는 2012년 2월 신설된 조항으로, 2012년 8월 시행되었다. 이에 따라 정보보유자는 2013년 8월까지 개인정보이용내역을 정보주체에게 최초통지를 수행해야하는 의무가 부여되었는데, 많은 정보통신서비스제공자가 2013년 8월 일제히 통지를 실시함에 따라, 일시에 수많은 본인정보 이용내역의 통지를 받게 된 정보주체들이 본인의 정보가 해킹 당한 것은 아닌가 의심하는 사례가 발생한 바 있다[12].

2.4 금융지주회사법

세계 금융시장은 국제화의 진전 및 정보통신 기술의 발달과 규제 완화 등으로 급속한 환경변화를 맞고 있으며, 주요 금융기관들은 금융지주회사 방식을 활용하여 인수합병을 통한 대형화 및 이종 금융기관간 통합에 의한 겸업화 등으로 환경변화에 적극 대응하고 있는 바, 우리나라도 이러한 세계적인 금융환경의 흐름에 따라 대형화 및 겸업화를 통해 경쟁력을 강화하고 지배구조개선 및 금융구조조정을 촉진하고자 2000년10월 금융지주회사법이 제정되었다[13].

금융지주회사법에서는 금융지주회사등간의 고객정보공유의 필요성을 인식하고 금융지주회사그룹의 시너지효과 및 그룹전체의 경영효율성 제고를 위하여 동일한 금융지주회사에 속하는 회사 상호간에는 신용정보의 이용 및 보호에 관한 법률 등의 적용을 배재하여 고객의 동의 없이도 정보를 제공할 수 있도록 허용하고 있다. 다만, 금융지주회사내 정보제공으로

인한 고객정보의 침해, 남용을 방지하기 위한 보완장치(이하 고객정보 제공절차)를 별도로 마련하고 있는데 주요 내용은 다음과 같다.

가. 금융지주회사등간 고객정보 공유는 내부경영관리 목적으로 제한(영업목적의 공유 금지)
나. 금융지주회사등은 고객정보관리를 위한 고객정보 관리인을 임원으로 선임
다. 고객정보에 대한 요청·제공 시 고객정보관리인의 승인을 얻을 것
라. 정기적인 점검 수행 후 감독기관에 보고
마. 고객정보에 대한 암호화 제공, 고유식별정보 변환, 분리보관 등의 기술적 조치 이행
바. 그룹사간 고객정보 제공 시 그 내용을 연1회 이상 정보주체에게 통지(무조건적 자기정보접근권)
사. 고객정보 제공내역을 조회할 수 있는 조회시스템 구축(조건적 자기정보접근권)

금융지주회사법상 자기정보접근권 보장에 대한 내용은 각각 법 제48조의2 제4항 및 금융지주회사법 시행령 제27조의2 제3항에서 규율하고 있다.

시행령 제27조의2 제3항에서는 조건적 자기정보접근권 보장에 관한 사항으로 고객정보 제공내역 조회시스템 구축하여 금융지주회사 그룹사간 고객정보가 제공된 내역에 대해 정보주체가 조회할 수 있도록 하고 있다. 이는 신용정보법 제35조에서 규율하고 있는 조건적 자기정보접근권 보장방식과 그 내용이 본질적으로 동일하다.

법 제48조의2 제4항에서는 무조건적 자기정보접근권을 규율하고 있다. 법 제48조의2에서는 금융지주회사 및 그 자회사, 손자회사, 증손회사(이하 "그룹사")간 고객정보가 제공된 경우 그 내역에 대해 무조건적으로 통지하도록 하고 있다. 해당 의무는 2014년 카드사 정보유출사고 이후 고객정보관리 강화 필요성에 따른 법 개정에 따라 새로이 부과된 것으로, 이는 정보통신사업자의 정보유출에 따른 정보통신망법 제30조의2의 정보통신사업자의 통지의무 부과와 배경이 유사하다. 차이점은 정보통신망법은 개인정보의 제공내역을 포함하는 전체 이용내역을 통지하도록 하고 있지만, 금융지주회사법에서는 제공내역에 대해서만 통지하도록 하고 있다는 점이다. 이는 본질적으로 금융지주회사법상 개인정보의 이용목적은 내부경영관리업무로 제한되어 있으며, 금융지주회사 그룹사간의 개인정보 제공·이용과 관련된 사항만을 그 규율범위로 하고 있기 때문이다.

법 제48조의2에 따라 금융지주회사 그룹사간 고객정보를 제공한 경우에는 시행령 제27조의2제3항에 따라 고객정보를 제공하는 자, 고객정보를 제공받는 자, 고객정보의 제공목적, 고객정보의 제공항목에 대해 연1회 이상 정보주체에게 통지하도록 하고 있으며, 우편, 전자우편, 문자메시지를 그 매체로 활용하도록 하고 있다.

III. 자기정보접근권 보장 관련 해외 사례

3.1 경제협력개발기구(이하 "OECD")

IT기술의 발전에 따라 데이터 처리의 자동화가 가속화되고, 막대한 양의 데이터가 국가간 이전될 수 있는 환경이 조성됨에 따라, OECD에서는 개인정보 데이터와 관련된 프라이버시 보호에 대한 고려가 필요하다고 인식하게 되었다. 또한 IT기술 발전에 따른 국가간 데이터 교류의 중요성이 높아지고 그 수요가 증대되는 과정에서, 국가간 상이한 개인정보보호 규제로 인한 데이터의 적절한 교류가 제한되지 않도록 OECD회원국간 개인정보보호 규제를 조화시키면서, 개인의 정보보호 권리를 보장하기 위하여 OECD에서는 1980년 프라이버시 가이드라인(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 이하 "OECD가이드라인")을 채택하였다[14].

본 가이드라인은 개인정보의 수집 및 처리 볼륨 증가, 개인정보 분석 범위 확대, IT 기술 발전에 따른 개인정보 이용의 가치 증대 등 여러가지 시대적 변화를 고려하여 2013년에 개정된 바 있다.

OECD가이드라인에서도 정보주체의 자기정보접근권 보장을 위한 원칙이 존재하는데 바로 개인참여원칙이 그것이다. OECD가이드라인의 해설에서는 개인참여원칙을 개인정보보호와 관련된 가장 중요한 안전장치로 간주한다고 설명하고 있다[15]. 관련하여 정보주체가 정보보유자와 합리적인 수준의 커뮤니케이션을 하는 기준에 대해, 정보주체가 본인정보의 열람을 요청 시 그 요구를 충족시키는데 소요되는 기간은 처리하는 데이터의 성질, 기타 거리 등 정보주체에게 정보를 전달하는데 소요되는 물리적 시간 등을 고려하도록 하고 있다.

또한 정보보유자가 정기적으로 정보주체에게 정보를 제공하고 있는 경우에는, 정보주체의 자기정보와

관련된 열람요청에 응할 의무에서 제외될 수 있다.

OECD가이드라인 및 관련 해설에서는 무조건적 자기정보접근권 보장과 관련된 정보보유자의 의무는 규율하고 있지 않다.

3.2 유럽연합(이하 "EU")

EU에서는 개인 프라이버시의 보호와 유럽연합 회원국들간의 개인정보의 자유로운 유통에 대한 조화를 목적으로 1995년 '개인데이터 처리에 관한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 지침(European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movemnet of such data, 이하 "EU지침")을 제정하였다[16]. EU지침은 개인정보보호라는 기본권을 수호하였으나, EU회원국이 개인정보보호법을 상이하게 집행함으로써, 복잡성과 법적 불확실성, 그리고 행정적 비용이 발생하였다[17]. 이러한 배경에 따라 EU에서는 회원국들의 불일치한 자국법을 대체할 범유럽 데이터 보호법을 제정하고, 소셜네트워크, 클라우드 컴퓨팅 등 IT기술 발전에 따른 시대의 변화를 반영하기 위하여 2012년부터 개인정보보호규정(General Data Protection Regulation, 이하 "GDPR")제정에 대한 논의를 하기 시작하여, 2016년 5월 그 최종안이 공식적으로 공표되었다. GDPR로 인해 기존 법적 구속력이 없었던 EU지침(Directive)은 법규적 효력을 가진 규정(Regulation)으로 대체되어 유럽연합 회원국 전체가 2년간의 유예기간을 거쳐 2018년 5월 25일부터 적용받게 될 예정이다. GDPR은 기존 EU지침과 비교하여 정보주체의 권리보장을 대폭 강화하였는데, 그 중 자기정보접근권 보장과 관련된 사항은 주로 2장에서 규율되고 있으며 주요 내용은 다음과 같다.

3.2.1 정보주체로부터 개인정보 수집 시 고지의무

GDPR에서는 제13조에서 정보주체로부터 개인정보 수집 시의 고지의무를 규율하고 있다. 정보보유자는 정보주체로부터 개인정보를 수집 시, 정보를 수집하는 시점에 '정보보유자 신원 및 대표자', '정보보호담당자 연락처', '정보수집 목적 및 관련 법적 근거', '제3자 제공 시 정보를 제공받는자', '정보보유기간', '정보의 접근, 정정, 삭제, 처리제안을 요청할 수 있는 권리', '감독기관에 민원을 제기할 수 있는 권리', '프로파일링 존재 여부' 등을 정보주체에게 고지하여야 한다.

여기서 '프로파일링' 이란 정보주체의 특정 측면을 평가하기 위하여, 특히 정보주체의 직업, 경제력, 건강, 관심사 등을 분석 또는 예측하기 위해 이루어지는 개인정보에 대한 모든 형태의 자동화된 처리를 말한다.[18]. 이는 EU지침에서는 존재하지 않았던 개념으로, IT기술 발전에 따라 고도화된 개인정보 처리에 따른 마케팅, 개인화 서비스 등이 가능해짐에 따라, GDPR에서 이러한 시대적 변화에 맞는 개인정보보호 정책을 제시하기 위하여 도입한 개념이다.

이 외에도 이용 목적이 변경되는 경우, 해당 변경된 목적에 따른 처리 전에 해당 사실을 정보주체에게 고지하도록 하고 있다.

다만, 단서조항에 따라 상기 모든 고지의무는 정보주체가 이미 그 내용을 알고 있는 경우에는 적용되지 아니한다고 예외를 두고 있다.

3.2.2 정보주체 이외로부터 개인정보 수집 시 고지의무

GDPR 제14조에서는 정보보유자가 정보주체 이외로부터 개인정보를 수집 시의 고지의무를 규율하고 있다. 정보보유자는 정보주체 이외로부터 개인정보를 수집 시에도 정보주체에게 관련 사항을 고지해야할 의무가 있다. 고지해야할 항목은 정보주체로부터 수집 시 고지해야하는 내용에 추가하여 정보의 수집 출처에 대해 추가적으로 고지해야한다.

고지 기한은 정보 수집한 이후 합리적인 기간 내 하도록 하고 있으나, 개인정보가 처리되는 환경까지 고려하여, 최대 1개월 이내에 하도록 하고 있다.

또한 수집된 개인정보가 정보주체와의 직접적 커뮤니케이션 목적으로 사용된다면, 그 커뮤니케이션 시점에 고지를 하도록 하고 있다.

마지막으로, 상기 모든 고지 의무는 '정보주체가 이미 그 내용을 알고 있는 경우', '해당 고지가 불가능한 것으로 판명된 경우', '심각하게 불공평한 노력이 수반될 경우', '해당 통지가 정보처리 목적 달성을 제한할 가능성이 높은 경우'에 대해 예외가 존재한다.

3.2.3 정보주체의 접근 권리

GDPR 제15조에서는 '정보주체의 접근 권리'를

규정하고 있다. 본 조에 따라 정보주체는 정보보유자가 보유하고 있는 본인의 개인정보 및 '정보처리 목적', '정보이용 항목', '개인정보의 제3자 제공에 관한 사항', '정보이용기간', '정보주체의 권리' 등에 관한 정보에 대해 접근할 수 있는 권리를 가진다.

무조건적 자기정보접근권은 GDPR 제14조에서 규율하고 있는 '정보주체 이외로부터 개인정보 수집 시 고지의무'에서 부여하고 있다. 이는 국내 개인정보보호법의 정보주체 이외로부터 개인정보 수집 시 통지의무와 유사한데, GDPR에서는 국내 개인정보보호법과 달리 해당 의무가 적용되는 정보보유자의 범위 및 통지 방법을 특별히 정하고 있지 않다.

또한 정보주체가 이미 그 내용을 알고 있는 경우, 심각하게 불공평한 노력이 수반될 경우, 해당 통지가 정보처리 목적 달성을 제한할 가능성이 높은 경우로 하여금 예외를 두고 있다. 여기서 불공평한 노력이 수반될 경우에 대해 공공 이익, 학술연구, 통계 목적을 그 특별한 사례로 들고 있다.

3.3 미국

미국은 개인정보보호에 관한 사항을 포괄하는 개인정보보호기본법은 없지만, 각 영역별로 개인정보보호를 위한 규제가 존재한다. 미국은 프라이버시를 헌법적인 권리로 보장하고 있음에도 불구하고, 포괄적이고 체계적인 개인정보보호 관련된 일반법이 존재하지 않는다. 이에 대신하여 사회적인 변화나 기술 진보에 따라 개별 영역에서 개인정보보호를 위한 개별법적인 접근방식으로 대응하고 있으며, 이는 탈 중심적 권위에 대한 선호, 사적 부문의 월권보다 정부의 월권에 관한 더 큰 우려 등 미국법적 전통에서 기인하는 것이라 할 수 있다[19][20].

이와 같이 미국의 개인정보보호와 관련된 법은 공공·민간 부문을 통합하지 않고 분리된 입법모델을 채택하고 있어, 각 영역에 적용되는 법체계를 파악하기 위해서는 대표적인 공공부문의 프라이버시법을 살펴볼 필요가 있다[21].

미국의 공공부문에서의 개인정보 보호에 관한 입법적 노력은 대단히 오래 동안 지속되어 왔지만, 궁극적으로 정부기관에 의하여 수집되는 정보의 관리에 대한 책임을 인정하고 이를 통제하기 위한 개인의 권리를 인정하기 위해 제정된 1974년 프라이버시법제정작업의 급속한 진전은 1972년 워터게이트 사건 동안 발생되었던 닉슨 행정부의 개인정보의 자의적인 활용의 폐해를 막기 위해 촉발되었다. 프라이버시법 원안은 연방프라이버시위원회의 규정을 두고 민간부문에의 적용도 상정하고 있었지만, 이러한 규정들은 삭제되고 이후 몇 차례의 논의와 토론으로 가다듬어진 후 포드 대통령이 프라이버시법에 1974년 12월 31일 서명하고 1975년 9월 27일부터 시행되었다. 프라이버시법의 핵심은 공공부문에서의 개인프라이버시의 보호를 주된 관심사로 하며, 구체적으로는 연방기관으로부터 개인의 프라이버시를 보호하기 위한 내용을 두고 다른 한편 연방기관이 보유하고 있는 개인의 기록에 관련 당사자가 접근할 수 있는 권리를 부여하고 있다는 점이다[22].

프라이버시법에서의 자기정보접근권은 미국 시민의 개인정보를 보유하고 있는 기관이 정보주체의 요청에 따라 정보주체 및 그 동반자에게 개인정보의 조회를 허용함으로써 보장하고 있다. 정보주체는 본인의 정보에 대한 정정을 요구할 수 있으며, 요청을 받은 기관에서는 정보주체의 정정요청의 이행을 거부하는 경우 그 사유를 안내하도록 하고 있다. 만약 기관의 정정 이행거부에 대해 정보주체가 불복할 경우, 정보주체는 기관을 상대로 소송을 제기할 수 있도록 하고 있다.

이는 조건적 자기정보접근권으로서, 개인정보의 정정에 대해 많은 부분을 할당하고 있는데, 국내와 유럽과는 달리 삭제 및 처리금지권은 보장하고 있지 않다. 이는 프라이버시법이 공공영역에 대한 규율임에 따라 그 대상이 국가기관으로서, 개인정보의 삭제 및 처리금지권에 대한 보장은 정상적인 국정업무 수행에 지장을 줄 수 있기 때문으로 판단된다.

프라이버시법에서의 무조건적 자기정보접근권은 '기관의 의무사항들'에서 규율되는데, 개인정보가 강제적인 법적 절차에 따라 공공정보로 변경되어 제3자의 접근이 가능해지는 경우에는 정보주체에게 알릴 수 있도록 합당한 노력을 기울이도록 하는 수준으로 규율하고 있다.

3.4 일본

일본은 1980년 OECD프라이버시 가이드라인이 채택된 이후, 1981년부터 공공 및 민간부문의 개인정보보호에 관한 법제 정비를 검토하기 시작하였다. 공공부문에서는 1988년 "행정기관이 보유하는 전자계산기 처리에 관련된 개인정보의 보호에 관한 법률"이 제정되었고, 민간부문에서는 일부 업계에서 자발

적으로 지침 또는 가이드라인을 제정하여 자율규제를 시행하고 있었다. 민간부문의 개인정보보호법제 정비 요구는 1995년 EU의 "개인정보보호지침"의 채택 이후 EU와의 통상 협상 과정에서 EU수준의 개인정보보호법제의 필요성이 대두되고, 정보통신기술의 발달로 인한 개인정보 대량 유출 사건이 발생하면서 더욱 촉진되었다. 이에 따라 1998년부터 민간부문의 개인정보보호법 제정을 위한 검토가 시작되었고, 이후 민간부문과 공공부문을 포괄하는 개인정보보호법제의 정비를 목표로 논의가 진행되었다. 일본의 현행 "개인정보보호법"은 2003년 5월 30일에 공포되었고, 2005년 4월 1일부터 시행되고 있다[23].

일본 개인정보보호법에서 정보보유자는 정보주체의 요청에 따라 개인정보의 열람, 정정, 삭제, 처리정지를 수행할 의무가 있다. 이는 국내의 개인정보보호 관련 법상의 정보주체의 권리와 유사하며 조건적 자기정보접근권에 해당한다.

반면 무조건적 자기정보접근권을 규율하는 조항은 존재하지 않는다. 개인정보의 수집과 관련하여, 개인정보를 취득했을 경우에는 그 이용목적을 통지하거나 공표하도록 하고 있으므로, 미리 공표한 경우에는 사후 통지가 필요 없다.

또한 개인정보의 제3자 제공과 관련하여서도 고객동의를 받지 않는 경우의 예외사항으로 Opt-out방식을 인정하면서 사후 통지 의무를 부여하고 있으나, 쉽게 알 수 있도록 하는 경우로 하여금 대체가 가능하므로 이는 무조건적 자기정보접근권이라고 볼 수 없다.

IV. 무조건적 자기정보접근권 보장 관련 국내기업 법률 준수 사례

국내 개인정보보호 관련 법에서 요구하는 무조건적 자기정보접근권과 관련된 국내 기업들의 적용에 대해서는, 국내 금융지주회사들이 금융지주회사법 제48조의2 제2항에서 규율하고 있는 금융지주회사 그룹사간 고객정보 제공내역에 대한 통지의무를 적용한 사례를 통해 살펴보도록 하겠다.

해당 사례를 무조건적 자기정보접근권 방식의 규제에 대한 효과를 검증하기 위해서 이용할 경우, 표본집단의 규모가 커 그 결과값에 대한 신뢰도가 높으며, 사례의 적용방법에 있어서도 일반화가 가능하기 때문이다.

금융지주회사법에서 규율하는 무조건적 자기정보접근권의 대상은 내부 경영관리 목적으로 금융지주회사 그룹사간 개인정보가 제공된 모든 정보주체로, 해당 권리보장의 대상이 되는 정보주체의 수가 타 사례보다 많다는 점이다.

특히 본 연구에서 사례로 활용된 A금융지주회사의 경우에는 그룹사가 보유한 정보주체 수는 3천만명 이상으로, 국내 인구의 절반 이상이 포함되어 분석 결과에 대한 일반화가 가능하다는 점과 적용결과에 대한 접근성이 고려되었다.

금융지주회사법에서 요구하고 있는 무조건적 자기정보접근권 관련 사항을 요약하자면 다음과 같다.

Related Element of Notification	Included Contents
Subject for notification	Person whose information has been provided between group companies
Contents of notification	Company which provided personal information Companies which were provided with personal information Purpose of providing personal information Items of providing personal information
Media of notification	Mailing, e-mail, SMS
Period of notification	Once a year

이와 관련하여 금융지주회사감독규정에서는 통지의무이행 시 통합적 통지가 이루어지도록 노력하여야 한다고 명시하고 있다[24]. 이는 금융지주회사 그룹사간 고객정보 제공내역을 통지할 때 소속 그룹사들이 모두 개별적으로 통지를 수행할 경우, 동일 정보주체에게 전달되는 통지의 수가 과다해지는 상황이 발생할 수 있기 때문이다. 금융지주회사 그룹사들이 고객정보 제공내역을 통지함에 있어 그룹별로 그 제공내역을 통합하여 통지한다면, 소속된 그룹사의 수와 관계없이 그룹 내에서 발송되는 통지 횟수가 1회로 고정되므로 정보주체의 통지 과다수신을 예방할 수 있다.

본 통지의무를 수행하는 데 있어서 국내 금융지주회사 그룹들이 가장 고려한 부분은 각 금융지주회사 그룹별로 수천만명에 달하는 통지대상 고객 수와 통

지로 인해 발생하는 각종 민원 및 고객상담센터로 유입되는 문의였다. 각 금융지주회사들은 이에 공동으로 대응하기 위해 사전에 통지방법, 문구 등을 협의하였다.

사전 협의를 통해 각 회사들은 통지의무 이행시 미처 고려하지 못했던 사항을 점검할 수 있고, 서로 다른 금융지주회사 그룹간 통지 내용의 차이를 제거해 고객민원 및 문의를 감소시킬 수 있으며, 추후 관련 감독기관의 검사 및 제재에 공동대응할 수 있는 등 많은 이점을 얻을 수 있다.

다만 통지시점은 별도의 협의 없이 각 금융지주회사 그룹별로 각자 실시하기로 하였는데, 이는 금융지주회사 그룹간 상당한 비율의 고객 수가 중복되기 때문이다.

2016년 기준 금융지주회사법상의 고객정보제공내역에 대한 통지 의무를 적용받는 금융지주회사 그룹은 9개이며, 이 중 7개는 은행지주회사이다. 은행금융지주회사란 지배하는 그룹사 중 은행이 포함되어 있는 금융지주회사를 말하며, 국내 은행금융지주회사들의 계열사 중에서는 은행이 가장 많은 수의 고객을 보유하고 있다.

2016년 상반기 기준 국내 고객 수 기준 상위4개 금융지주회사 소속 은행 고객 수는 다음과 같다.

bank A	33 million	bank B	24 million
bank C	28 million	bank D	18 million
total	about 100 million (number of customers of each banks can be overlapped)		

* The figure shown here are approximate estimate only

상기 4개 은행 외 기타 은행을 감안하지 않더라도, 국내 총 인구수는 약 5,200만명이므로 1인당 평균 약 2개의 금융지주회사 소속 은행과 거래하고 있는 것으로 나타났다. 국내 총 인구 중에는 은행과 거래를 전혀 하지 않는 미성년자 등도 포함되므로, 이들을 제외한다면 1인당 거래 은행 수는 더욱 증가할 것이다.

특히나 생산활동에 종사하는 연령대에서는 은행뿐 아니라, 카드, 증권, 보험 등 다양한 금융상품을 소비하고 있다. 국내 대부분의 금융지주회사에서는 이러한 서비스를 제공하는 금융회사들이 그룹사에 포함되기 때문에, 금융지주회사 그룹간에는 상당한 비율의 고객이 중복된다.

금융지주회사들이 통지시점을 사전 협의하지 않은 이유는 이러한 중복고객에 대한 문의 또는 민원 유입을 예방하기 위함이다.

통지를 받은 고객이 해당 내용에 대해서 의문사항이나 불만을 갖게 될 경우, 이를 통지한 금융회사에게 문의하거나 민원 제기를 통해 이를 해소할 것이다.

하지만 해당 고객이 여러 금융지주회사 그룹들과 거래 중인 중복고객이라고 가정해 보자. 최초 통지를 받은 이후 다른 금융지주회사 그룹으로부터도 추가적으로 통지를 받게 되겠지만, 앞선 사전협의에 따라 금융지주회사 그룹간 통지 내용은 큰 차이가 없을 것이다. 따라서 추가적으로 받은 통지의 경우 관련된 의문사항이나 불만이 앞선 민원을 통해 해소되었을 가능성이 높다. 결론적으로, 가장 먼저 통지를 수행하는 금융회사가 타 회사와의 중복고객의 문의 및 민원을 해소해주게 된다.

이러한 이유로 인해 금융회사들로서는 타 금융회사와 비교하여 통지시기를 늦출수록 중복고객에 대한 문의 또는 민원이 감소되므로, 모든 금융지주회사 그룹들은 일정에 대한 사전 협의 없이도 자연스럽게 법상 통지기한 내 최대한 늦게 통지를 실시하는 계획으로 통일되었다.

그 결과, 모든 금융지주회사 그룹사가 그룹사간 고객정보 제공내역에 대한 최초 통지를 2016년 4월부터 2016년 5월에 걸쳐 실시하게 되었으며, 이는 정보주체들을 대상으로 짧은 기간에 과다한 통지를 제공하게 되는 결과를 낳았다. 이러한 결과는 당시 정보주체의 반응을 감안 시, 정보통신망법상 무조건적 자기정보접근권에 따른 통지에서도 유사하게 발생한 것으로 파악된다[12].

금융지주회사법에서는 시행령을 통해 통지 매체를 우편, 전자우편, 문자메시지로 제한하였다. 하지만 문자메시지에 담을 수 있는 내용의 양은 다른 매체 대비 제한적이므로 금융지주회사 그룹사간 고객정보 제공내역을 모두 문자메시지를 통해 전달하기는 불가능하다. 이에 금융지주회사법 시행령에서는 문자메시지를 활용하는 경우에는 고객정보조회시스템을 통해 그 조회사항을 조회할 수 있다는 사실을 알려주는 경우로 한정하였다[25].

이에 각 금융지주회사에서는 문자메시지에 각 회사별 고객정보조회시스템을 참조하는 인터넷 주소를 첨부하고, 정보주체가 직접 해당 인터넷 주소에 접속하여 스스로 조회하도록 하였다.

통지 매체별 발송에 소요되는 비용은 우편, 문자메시지, 전자우편의 순으로 높다.

법에서는 특별히 매체의 우선순위를 정하여 놓지 않았으므로, 당연히 통지를 수행하는 금융회사로서는 비용이 적게 소요되는 매체를 우선 선택하게 된다. 따라서 발송 대상 고객에게 전자우편 발송이 가능한 경우에는 전자우편을 발송하고, 전자우편 발송이 불가능한 경우에는 문자메시지 발송 가능여부에 따라 문자메시지를 발송한다. 결국 우편은 전자우편, 문자메시지 모두 발송 불가능한 대상에게만 발송된다. 이러한 매체선정 방법은 비용관점에서 가장 합리적이므로, 모든 금융지주회사 그룹에서 동일하게 채택되었다.

이렇게 통지를 실시한 결과에 대해서는 A금융지주회사 그룹의 사례를 통해 살펴보겠다.

통지 대상인 약 3천3만명의 고객 중 전자우편으로 및 통지한 고객 수는 약 1천5백만명, 문자메시지로 통지한 고객 수는 약 1천6백만명이었다. 우편으로 통지한 고객은 약 2백만명으로 나타났다.

반면 A금융지주회사가 발송한 전자우편에 대한 열람고객 수는 약 60만명으로 발송건수 대비 열람율은 약4.1%로 나타났다. 고객 1,000명당 해당 내용을 열람한 고객 수는 41명에 그친 것이다.

문자메시지를 받은 고객 중에서 직접 고객정보조회시스템에 접속하여 제공내역을 확인한 정보주체의 수는 해당 통지기간 중 약 700건으로 약 0.004%로 나타났다. 문자메시지를 발송 받은 10만명당 확인 고객 수는 약4명에 불과하여 통지 효과가 거의 없는 것으로 파악되었다.

우편의 경우에는 실제 정보주체가 해당 내역을 확인하였는지 여부를 확인하기 불가능하였다. 하지만 A금융지주회사 그룹에서 확인된 정보주체의 우편수령에 따른 문의 또는 민원 발생건수가 타 매체 대비 높지 않아 그 효과가 전자우편 및 문자메시지 대비 높다고 보기 어렵다고 파악된다.

결론적으로 이러한 통지 방식은 통지 열람 비율이 약2%에 불과하여(열람여부가 정확히 확인되지 않는 우편 제외), 그 효과가 대단히 낮은 것으로 파악되었다.

A금융지주회사 그룹은 통지에 따른 문의와 민원에 대응하기 위하여 주요 그룹사의 고객상담센터에 별도 상담인력을 배치하고, 정보보호 담당 책임자를 별도 대기하도록 하여 상담인력이 교육받지 못한 질문 및 민원에 대응하도록 하였다.

발생한 주요 문의사항은 '본인의 동의 없이 정보를 제공한 사실에 대한 문의' 및 '거래를 중단한지 오래되었음에도 제공된 사실에 대한 문의' 등이 있었으며, 요구사항에는 '개인정보 제공 중단 요구', '통지 중단 요구' 등이 있었다.

이 중 '개인정보 제공 중단 요구' 및 '통지 중단 요구'는 원칙적으로 정보주체가 본인의 개인정보와 관련된 자기정보결정권을 행사하는 방법 중 하나이지만, 관련 법에서는 명시적으로 이를 보장하고 있는 바가 없다.

'개인정보 제공 중단 요구'와 관련하여, 금융지주회사법에서는 내부경영관리 업무를 위해서는 정보주체의 동의나 의사와 무관하게 그룹사간 고객정보 공유를 허용하고 있다. 이는 국제기준 준수 등 그 목적 이행의 불가피성이 있기 때문이다. 이 외에도 내부경영관리 업무에 속하는 "신용위험 관리 등 위험관리와 내부통제" 및 "업무 및 재산상태에 대한 검사" 등은 모두 금융회사의 자산건전성 제고와 내부통제 절차의 보증 등 금융회사의 신뢰도 및 경쟁력 강화에 기여하여 정보주체에게 더욱 안심하고 금융회사와 거래할 수 있는 사회적 기반을 마련해 준다. 즉 정보주체의 권리보다 우선되는 공공의 이익 증대를 위해 부여된 사항이라고 볼 수 있다.

'통지 중단 요구'는 금융지주회사법에 따라 실시되는 통지에 대한 정보주체의 거부 요청이다. 법에서는 해당 요구 발생 시의 금융기관의 통지의무 예외 적용 사항에 대한 명시된 바가 없어, 이에 대한 해석이 필요하였다. 이에 따라 여러 금융지주회사가 공동으로 법무법인에 법률질의를 실시하고, 감독기관에도 관련 해석을 요청하였다.

법무법인에서는 본 사안과 관련하여 통지의무 적용 예외로 보는 것이 타당하다는 의견을 제시하였다.

그에 대한 첫 번째 주요 근거는 정보주체의 통지 거부 요청이 법에서도 통지 예외로 규정하고 있는 "통지할 수 있는 연락처 등 개인정보가 전혀 없는 경우" 와 유사하다는 점이다. 또한 이런 예외사유를 정한 해당 규정 취지에도 부합된다.

두 번째 근거는 동일한 목적에 따라 정보의 정확성·최신성 보장을 위해 반복적으로 고객정보를 제공할 경우 기존의 통지로 연1회 이상 하여야 하는 통지를 갈음할 수 있도록 하고 있다는 점이다. 고객의 예상 가능한 범위 내에서 고객정보를 제공하는 것은 통지의 필요성이 인정되지 않기 때문에 통지의 예외로 인정한 것이다. 마찬가지로 고객이 통지가 불필요하다고 요청한 경우에도 고객의 예상 가능성의 측면에서 통지의 필요성이 있다고 볼 수 없다.

마지막으로 정보주체인 고객이 원하지 않음에도 관련 사항을 매년 통지하도록 하는 것은, 정보주체가 개인정보의 이용(특히 '공개'를 포함)에 관하여 스스로 결정한 권리인 개인정보 자기결정권에 반한다고 볼 수 있다.

감독기관에서는 정보주체의 '통지 중단 요구' 에 대한 공식적인 답변은 없었다. 다만, 그러한 요청에 따른 통지의무 적용 예외에 대해 법률상 예외사항에 대해 명시된 바가 없으므로, 예외를 허용하면 안된다면 보수적 관점으로 해석하고 있는 입장이었으나, 이를 공식화하지 않아 추후 해석의 변경 여지를 남겨두었다.

V. 무조건적 자기정보접근권의 문제점

사례에서 확인된 정보주체 대상 통지를 통한 무조건적 자기정보접근권의 문제점은 다음과 같다.

5.1 낮은 목적달성 효과

A금융지주회사의 사례에서 확인된 통지내용에 대한 실제 접근고객의 수는 전체 통지 대상고객 수의 약2%로 나타났다.

본 결과를 통한 무조건적 자기정보접근권에 대한 효과의 일반화에 대해서는 다음과 같은 근거에 따라 가능하다고 판단된다.

첫 번째로, 국내에서 나타나고 있는 무조건적 자기정보접근권은 본 사례와 같이 전자우편, 우편, SMS, 전화 등의 방법을 선택하여 정보주체에게 개인정보의 처리와 관련된 사항을 알리도록 하는 방식으로 모두 유사하게 규율되고 있다.

두 번째로, 이를 이행하는 정보보유자들도 비용최소화를 위하여 전자우편 및 문자메시지를 우선순위로 하여 통지 매체를 선택하게 되므로, 통지 이행방안도 유사하게 적용된다.

마지막으로, 본 연구의 결과수치를 도출한 표본집단의 범위가 모집단(국내 인구)의 절반 이상으로 결과에 대한 신뢰도가 매우 높다.

결론적으로 무조건적 자기정보접근권 방식의 규제는 정보주체의 자기정보결정권을 보장하고자 하는 목적달성 효과가 매우 낮은 것으로 파악되었다.

5.2 정보주체의 의사 미 반영

무조건적 자기정보접근권 이행 사례에서 확인된 정보주체의 피드백으로는 '개인정보 제공 중단 요구' 및 '통지 중단 요구'가 있었다.

'개인정보 제공 중단 요구'의 경우, 금융지주회사법에서 규율하고 있는 고객정보 제공은 국제기준 준수 등의 공공 이익증대 목적에 따른 것이다. 따라서 정보주체의 의사와 무관하게 법에서 부여하고 있는 사항이다. 개인정보보호법상 ″법률상 의무를 준수하기 위하여 불가피한 경우″, "공공기관이 법률 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우", "명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우" 등에 대해서는 정보주체의 동의 없이도 수집 이용 및 제공을 허용하고 있는 사항과 그 목적이 유사하며, 그 중요성에 따라 정보주체의 요구와는 무관하게 이행되어야 하는 불가피성이 존재한다.

'통지 중단 요구'는 무조건적 자기정보접근권에 대한 정보주체의 거부 요청으로 '개인정보 제공 중단 요구' 와는 달리 공공의 이익 증대와 상충되는 부분이 없다. '통지 중단 요구' 는 정보주체 개별적으로 적용되는 사항으로, 개인의 해당 요구가 받아들여지더라도 타인의 무조건적 자기정보접근권에는 영향을 미치지 않기 때문이다.

또한 자기정보결정권이란 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리"로, '본인의 개인정보가 얼마나 이용되었는지에 대한 정보' 도 개인정보에 해당된다. 따라서 자기정보결정권 보장을 위해서는 본인의 정보이용내역에 대한 통지 수령여부에 대한 권한도 보장이 되어야 함이 마땅하다. 즉, 정보주체의 '통지 중단 요구'에 대한 제한은 오히려 정보주체의 자기정보결정권에 대한 침해로 볼 수 있다.

이와 관련하여 법무법인에서도 "고객이 원하지 않음에도 관련 사항을 매년 통지하도록 하는 것은, 정보주체가 개인정보의 이용(특히 '공개'를 포함)에 관하여 스스로 결정한 권리인 개인정보 자기결정권에 반한다고 볼 수 있다"는 해석한 바 있다.

5.3 중복 규제

마지막 문제점은, 현재 개인정보보호 관련 법에서

는 무조건적 자기정보접근권 외에도 개인정보보호를 위한 충분한 의무를 부과하고 있다는 점이다. 금융지주회사법은 금융지주회사 그룹사간의 고객정보의 제공 및 이용을 허용하고 있지만, 고객정보를 공유하는 과정에서 정보유출의 우려가 있으므로 고객정보 제공 절차를 통해 이에 대한 보안대책을 마련하고 있다.〔26〕.

고객정보 제공절차 외에도 금융지주회사법에서는 다음과 같이 정보보유자에게 개인정보 처리와 관련된 의무를 많이 부과하고 있다.

가. 고객정보에 대한 요청·제공 시 고객정보관리인의 승인을 얻도록 하고, 매분기 제반사항에 대한 점검 후 연1회 감독기관에 보고
나. 업무지침서를 제·개정 시 이사회의 승인을 득하고, 금융위원회에 보고
다. 고객정보취급방침을 정하고 이를 연1회 이상 정보주체에게 통지하거나 일간신문 등에 공고
라. 금융거래를 개시한 경우 거래상대방에게 정보취급방침을 교부·설명
마. 금금융거래를 개시한 경우 거래상대방에게 정보취급방침을 교부·설명

결론적으로 무조건적 자기정보접근권에 따른 통지 이외에도 정보주체가 금융지주회사 그룹사간 고객정보가 공유된다는 사실을 다양한 경로를 통해 인지할 수 있도록 정보보유자에게 충분한 의무를 부과하고 있다.

개인정보보호법과 정보통신망법상에서도 이미 정보보유자의 의무를 충분히 부과하고 있다.

정보보유자는 제공받은 개인정보를 제3자에게 또 다시 제공할 때 별도의 제공동의를 받아야 할 의무가 있고, 제공받은 목적 외의 용도로 이용할 수 없다. 이 정도의 규율이면 충분할 것으로 보이며, 여기에 옥상옥 구조를 쌓는다고 하여 보호수준이 더 이상 올라가지 않는다. 보호 정도도 일정한 수준을 넘어가면 더 이상 보호기능을 못하고 오히려 규제의 역할만 커지게 될 수 있다〔27〕.

해외의 경우에는, 정보보유자가 보유한 대부분의 정보주체를 대상으로 무조건적 자기정보접근권을 부여하도록 하는 규제는 존재하지 않았다.

OECD, 미국, 일본에서는 무조건적 자기정보접근권을 부여하는 규제가 없었다. 유럽에서는 GDPR를 통해 정보주체 외로부터 개인정보를 수집 시 정보주체에게 그 내용을 고지하도록 하는, 국내의 개인정보보호법상 무조건적 자기정보접근권과 유사한 규제가 존재한다. 하지만 해당 규제는 개인정보를 정보주체 이외로부터 수집하는 특별한 경우에만 해당되는 사항이며 GDPR은 2018년 5월 시행될 예정으로, 그에 따른 무조건적 자기정보접근권 이행 사례는 현재로서는 찾아볼 수 없다.

정보보유자의 존재근거인 사업영위 등의 목적에 따라 불가피성이 있는 정보처리에 대한 무조건적 자기정보접근권 방식의 규제는 해외에는 존재하지 않았으며, 오직 국내에만 존재하였다.

VI. 개선방안

사례에서 드러난 무조건적 자기정보접근권의 문제점은 다음과 같다.

가. 낮은 목적 달성 효과
나. 정보주체의 의사 미 반영
다. 중복 규제

이러한 문제점의 개선방안을 마련하기 위해서는, 무조건적 자기정보접근권이 발생한 원인에 대한 고려가 선행되어야 그에 합당한 개선방안도 마련할 수 있을 것이다.

금융지주회사법에서는 통지 의무 부과의 근거로 개인정보 유출방지 및 고객정보 보호를 명시하고 있다〔28〕. 또한 정보통신망법에서는 대규모 개인정보 유출사고가 발생하는 것을 방지하기 위한 실질적 정보보호체계 확립을 그 근거로 명시하고 있다〔29〕.

개인정보 유출방지와 고객정보 보호, 정보보호체계 확립은 모두 정보주체의 자기정보결정권 강화로 귀결된다. 따라서 무조건적 자기정보접근권의 궁극적인 목적은 정보주체의 자기정보결정권 강화로 볼 수 있다. 또한 세부적인 목적은 각 법률에서 무조건적 자기정보접근권 관련 통지 내용을 정보주체에게 정확히 전달하는 것이라고 볼 수 있다.

다만, 앞서 문제점에서 설명한 바와 같이 현재 법체계에서는 무조건적 자기정보접근권 외에도 개인정보의 수집·이용·제공과 관련된 내용을 정보주체가 인지할 수 있도록, 정보보유자에게 개인정보의 수집 이전 단계에서부터 많은 의무를 부여하고 있다. 그러한 상황에서 무조건적 자기정보접근권과 같은 중복 규제가 계속 생기는 것은, 개인정보의 수집 이전 단계에서 부여된 의무들이 실제 적용되는 과정에서 그 목적

을 충분히 달성하고 있지 못하는 것으로 판단되기 때문일 것이다.

따라서 본 논문에서는 무조건적 자기정보접근권에서 드러난 문제점을 개선하면서 정보주체에게 개인정보의 수집·이용·제공 관련 내용을 보다 명확히 인지시키기 위하여, 개인정보 수집 이전 단계에서 개인정보 처리와 관련된 안내 및 동의절차를 강화하는 한편, 무조건적 자기정보접근권은 배제하도록 하는 방안을 제시한다.

일반적으로 개인정보 수집 이전 단계에서는 정보주체와 정보보유자간 양방향 커뮤니케이션이 가능한 경우가 많다. 오프라인에서는 정보주체와 정보보유자가 대면 커뮤니케이션을 하게 되며, 온라인에서도 정보보유자와 정보주체간 전자적 매체를 통해 정보전달 및 피드백이 이루어지는 양방향 커뮤니케이션이 수행된다.

이와 같이 양방향 커뮤니케이션이 가능한 개인정보 수집 이전 단계에서는 일방향으로만 정보가 전달되는 무조건적 자기정보접근권이 이행되는 시점보다 정보주체가 전달 내용을 인지할 수 있는 기회가 더 많이 보장된다.

정보주체로서는 능동적 선택상황에 직면하게 되므로, 안내되는 개인정보 수집·이용·제공 안내 사항에 더욱 주의를 기울일 수 있으며, 관련 의문사항 등에 대해 정보보유자에게 즉각 표출할 수 있기 때문이다.

이러한 상황에서는 자기정보접근권이 자연스럽게 보장될 수 있으므로, 무조건적 자기정보접근권을 문제점인 '낮은 목적 달성 효과'를 개선할 수 있다.

또한 개인정보 수집 이전 단계에서는 고객의 의사를 반영할 수 있는 기회를 자연스럽게 제공하므로, 무조건적 자기정보접근권상의 문제점인 '정보주체 의사 미 반영'을 개선할 수 있다.

개인정보보호법 및 정보통신망법상의 개인정보 수집 이전 단계에서의 동의 절차는 그 자체로 정보주체의 의사를 반영한다. 정보주체는 본인의 개인정보 수집·이용에 대해 사전에 동의 또는 거부할 수 있기 때문이다. 계약체결 및 이행에 필수적인 개인정보의 수집·이용에 대해서도 정보주체는 계약체결과 개인정보의 수집·이용 거부권 행사간의 개인적 선호도에 따른 선택을 할 수 있기 때문에, 정보주체의 의사가 반영된다.

금융지주회사법에서도 금융거래 개시 시점에 '정보취급방침'에 대해 설명 하도록 되어 있다. 본 설명은 동의절차와는 달리 정보주체의 관련 거부권이 부여되지 않고 있다. 다만, 이 시점에서 정보주체는 정보보유자와 양방향 커뮤니케이션을 통해 관련 근거 및 세부적인 내용을 설명 받고 의문을 해소할 기회를 부여받는다. 더 나아가 금융지주회사법에서 보장하고 있는 금융지주회사 그룹사간 고객정보 제공에 대한 정보주체의 거부는 정보주체 및 금융회사로부터의 법개정에 대한 요구로 이어질 수도 있다.

마지막으로 개인정보 수집 이전 단계에서의 절차를 강화하고, 무조건적 자기정보접근권을 배제하게된다면 자연스럽게 '중복 규제' 도 해소된다.

이상과 같이 무조건적 자기정보접근권에서 나타난 문제점을 해결하기 위하여 개인정보 수집 이전 단계에서의 안내 및 동의절차를 강화하는 방향을 제시하였지만, 그 세부적인 방법에 대해서는 별도의 연구가 필요하다.

현재 개인정보 수집 이전 단계의 동의제도는 정보주체가 자신의 정보에 대해 통제권을 가진다는 의미에서 개인정보자기결정권을 보장하기 위한 필수적인 요소라고 할 수 있다. 하지만 동의 항목이나 동의내용이 지나치게 복잡하고 많아 이용자가 동의사실과 내용을 충분히 인지하지 못하거나 아예 그러한 내용을 확인하지 않고 동의를 해 버리는 등의 문제점도 존재한다[30].

다만 이러한 문제점은 비단 개인정보보호 관련 법만이 아니라 기타 계약관계에 얽혀있는 다양한 법률상의 규제의 일부분으로써 존재하므로, 개인정보보호 관련 법만의 개선으로 완전한 해결이 되기는 어렵다고 판단된다.

가령 계약체결 시 개인정보 수집·제공에 대한 정보주체의 사전 동의는, 계약 또는 약관에 대한 동의, 혹은 기타 신용정보조회 등 계약체결에 수반되는 각종 절차상의 일부분으로서 존재한다. 따라서 계약 체결 전반에 걸친 모든 제도가 함께 고려되지 않는다면 실질적 개선효과가 없이 절차적 비효율만 낳는 규제가 생길 수 있다.

현재의 무조건적 자기정보접근권상의 비효율성 역시 그 자체만의 문제라기보다는, IT기술발달에 따른 개인화된 상품 마케팅 등 지나친 정보전달의 범람과 같은 사회적 현상에도 그 원인이 있는 것과 맥락이 같다.

다만, 본 논문에서 제시한 개선 방향에 따라 보다 넓은 범위에서 개인정보보호 관련 정책에 대한 개선 검토가 이루어진다면 실효성 있는 개선안이 도출될 것으로 기대된다.

VII. 결 론

본 논문에서는 무조건적 자기정보접근권과 관련된 국내 법 및 해외 규제 사례를 살펴보고 국내 기업의 준수사례를 통한 문제점을 분석하였다.

개인정보보호와 관련하여 그 어떠한 정보주체의 자기정보결정권 강화를 위한 개선책도 정보보유자의 적극적인 의지가 뒷받침되지 않는다면 또 하나의 형식적 관행으로 변질될 소지가 많다.

이를 근본적으로 개선하기 위해서는, 정보주체 개개인이 본인이 가진 자기정보결정권을 인지하고 적극적으로 행사하는 사회적 분위기가 조성되어야 한다.

이런 분위기 속에서 정보보유자도 정보주체의 자기정보결정권에 대한 중요성을 인식하여, 개인정보보호 문화 성숙도가 높아질 수 있다.

이를 위해서 본 논문에서는 개인정보의 수집 이전 단계에서 개인정보 처리와 관련된 안내 및 동의절차를 강화하는 한편, 무조건적 자기정보접근권은 배제하는 방향으로의 개선안을 제시하였다.

본 논문에서 제안한 방향대로 개선되기 위해서는 본 연구에서 확인되지 못한 효과검증을 포함한 보다 넓은 분야에서의 많은 연구가 필요하겠지만, 본 논문이 정보주체의 자기정보결정권에 대한 인식이 확대될 수 있는 계기를 마련하고, 개인정보를 소중한 자산으로 여기는 사회적 풍토를 조성하는데 도움이 되기를 바란다.

References

〔1〕 Constitutional Court of Korea 2005.5.26. 99 heonma 513 pp. 1, 2005

〔2〕 Sang-Myeong Lee, "The study on the constitutional basis of the right to informational self-determination", Public Law Korean public Law Association vol. 36, No. 3, pp. 225-226, Feb. 2008

〔3〕 Tae-Hyun Kim, "Constitutional Consideration of Personal Information Protection Regulations", pp. 15-16, 2003

〔4〕 Sang-Myeong Lee, The same paper as 〔2〕, pp. 228

〔5〕 Kun-Bo Lwon, "Personal Information Protection and the Personal Information Control Right", Kyungin Publishing, pp. 120, 2005

〔6〕 FSC, "Big change of personal Information protect regulation in finance sector", press release, pp. 1, Apr. 2016

〔7〕 Tae-Eon Koo, "Status and Improvement of the Legal System about the Transfer of Personal Information Abroad", Gachon Law Review Vol6. No.1, pp. 281, Mar. 2013

〔8〕 Seong-Koo Cheong, "The study and Issues of the Law concerning the Utilization and Protection of the Credit Information", The korean Journal of Security Law, Vol. 2, No. 2, pp. 1, 2001

〔9〕 Act No.13216, "Use And Protection of Credit Information Act", Reason for amendment , Mar. 2015

〔10〕 Act No.3848, "Act on the Expansion and Promotion of the Use of Information and Communication Network", Reason for legislation, Jan. 1987

〔11〕 Chul-Wan Kim/Min-Young Lee, "A study on the Legislation for Internet Personal Information Protection", Preface, Dec. 2000

〔12〕 Kyung-Ho Son, "flustered by email containing personal information usage record", ZDNet Korea, Aug. 2013

〔13〕 FSS Supervision Coordination Dep , "Explanation for the Financial Holding Companies Act", pp. 7, Dec. 2003

〔14〕 OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", Preface, 1980

〔15〕 OECD, "OECD Privacy Framework" EXPLANATORY MEMORANDUM, pp. 58, paragraph13, 2013

〔16〕 EU, DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October. 1995, article1, CHAPTER 1, 1995

〔17〕 EUROPEAN Commission, Questions and Answers - Data protection reform(http://europa.eu/rapid/press-release_MEMO

-15-6385_en.htm), 2015
〔18〕 EU, Regulation 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 April 2016, (4) Article 4, Apr. 2016
〔19〕 Dae-kyeong Jeong, "Comparative study of the privacy information protection policy", Journal of The Korea Institute of Information Security and Cryptology, pp. 993, Aug. 2008
〔20〕 Sang-Kyung Lee, "A study on the Legislative Scheme and the Current status of Personal information Protection of the United States", pp. 2, Aug. 2012
〔21〕 Sang-Kyung Lee, The same paper as 〔31〕, pp. 3
〔22〕 Sang-Kyung Lee, The same paper as 〔31〕, pp. 4
〔23〕 KCC, "Analysis for Legislation and Supervision System on Private Information Protection in EU and Japan", pp. 72 - 73, Dec. 2014
〔24〕 "Regulation on Supervision of Financial Holding Companies", No. 2015-45, Article 24-2 (7), Dec. 2015
〔25〕 Presidential Decree No. 26816, "Enforcement Decree of the Financial Holding Companies Act", Article 27-2 (5), Dec. 2015
〔26〕 FSS Supervision Coordination Dep, The same explanation as 〔23〕, pp. 14
〔27〕 Kyung-Hwan Kim, "Explanation for Amendment of the Personal Information Protection Act", http://blog.naver.com/n_privacy/220674006349, Apr. 2016
〔28〕 Act No.12713, "Financial Holding Companies Act", Reason for amendment, Nov. 2014
〔29〕 Act No.11322, "Act on Promotion of Information and Communication Network Utilization and information Protection", Reason for amendment, Aug. 2012
〔30〕 KCC, "A study on Agreement Procedure Improvement for Personal information Collection and Introduction of Personal Information Security Management Level", Summary, Dec. 2014

〈저자소개〉

배 진 호 (Jin-ho Bae) 정회원
1990년 8월: 경북대학교 통계학과 졸업
1990년 5월~1998년 9월: 대동은행 전산부
1998년 10월~2010년 7월: KB국민은행 전산정보부
2010년 8월~2013년 7월: KB금융지주 IT기획부 팀장
2013년 8월~2014년 12월: KB국민은행 IT운영부 팀장
2015년 1월~현재: KB금융지주 정보보호부장 겸 CISO
〈관심분야〉 정보보호, IT