Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.4, August 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.4.781

개인정보보호 수탁사 관리체계 강화 방안 연구*

강 태 훈,† 임 종 인‡
고려대학교 정보보호대학원

A Study on Consigned Party Management System Enhancement for Personal Information Protection*

Tae-hun Kang,† Jong-in Lim‡
Graduate School of Information Security, Korea University

요 약

오늘날 기업들은 비용절감, 업무의 효율성, 서비스 품질 향상 등의 이유로 외부 기업 또는 개인사업자에게 개인정보 처리 업무를 위탁 운영하는 경우가 증가하고 있다. 하지만, 개인정보 처리 업무 위탁 즉, 수탁사가 증가할수록 제공되는 개인정보의 종류와 량이 증가하며, 이에 따른 관리 포인트와 보안 위협도 함께 증가하게 된다. 따라서, 본 연구에서는 개인정보 처리 업무 위탁 시 준수해야 할 법률사항을 분석하고, 현재 개인정보 처리 업무를 위탁 받아 사업을 진행하는 수탁사들의 개인정보보호 수준 분석 및 문제점을 도출하여 기업이 개인정보 처리 업무 위탁에 있어서 개인정보를 보호하고 수탁사들을 효과적으로 관리·감독할 수 있는 방안에 대하여 제안하고자 한다.

ABSTRACT

Nowadays, it is increasing that corporates consign tasks related to the personal information processing to the consignees for efficiency and quality improvements and cost reductions. As the consignments are increased, there are increases on types and amounts of personal information. Therefore, the needs on the information managements and the security threats are increased. This report will analyze the laws that consignors and consignees should follow. Moreover, it identifies issues and analyzes the current levels on consignees in terms of the personal information protection so that the consignors can come up with the best and efficient way to monitor the consignees when they consign the personal information processing tasks.

Keywords: Personal Information Protection, Consigned Party

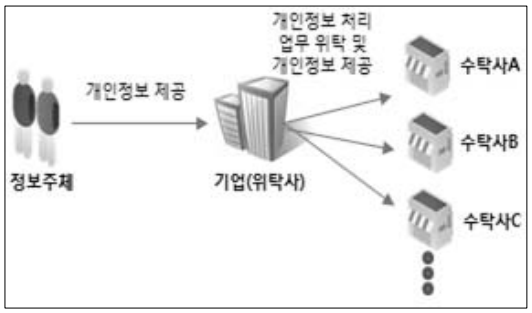
I. 서 론

개인정보침해신고 상담건수는 122,215건(2011년), 168,801건(2012년)[1], 해킹사고 처리건수는 11,690건(2011년), 19,570건(2012년)[2]으로 해마다 크게 증가하고 있으며, GS칼텍스, 옥션, SK커뮤니케이션 개인정보 유출 사건 등과 같이 대량의 개인정보가 유출되는 사건 또한 지속적으로 발생하고 있다. 끊임없이 발생하는 개인정보침해 및 해킹사고로 인해 개인정보보호법이 발효되고 정보통신망 이용 촉진 및 정보보호 등에 관한 법(이하 정보통신망법)이 개정되는 등 관련 법률은 한층 강화되었다. 그 결과 기업들은 내외부의 불법적 행위로부터 개인정보의 유출을 방지하고 법적 준거성을 확보하기 위해 정보보호 관리체계를 구축하고 DRM, DLP, DB암호화 등 다양한 보안솔루션을 도입하고 있다. 이와 같은 기업의

접수일(2013년 5월 28일), 수정일(2013년 7월 8일), 게재확정일(2013년 7월 22일)
* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 IT융합 고급인력과정 지원사업의 연구결과로 수행되었음 (NIPA-2013-H0301-13-3007).
† 주저자. acelucifer@korea.ac.kr
‡ 교신저자. jilim@korea.ac.kr(Corresponding author)

보안 강화 활동은 기업 자체의 개인정보보호 수준을 향상시키고 고객의 신뢰성을 확보하는데 크기 기여하였다. 하지만, 개인정보의 라이프 싸이클 관점에서 본다면 수집, 저장, 파기 영역의 보안 수준은 향상되었지만 이용 및 제공 영역에서는 여전히 보안위협이 존재한다고 할 수 있다. 이는 기업들의 개인정보의 이용 및 제공 구조와 개인정보 유출 사고를 통해 확인 할 수 있다.

우리나라 기업들의 개인정보 이용 및 제공 구조를 살펴보면, 기업들은 정보주체로부터 수집한 개인정보를 자사 서비스에 이용하고 수집된 개인정보를 분석하여 미래의 수익 모델에 반영하는 등 다양한 형태로 활용하고 있다. 이와 동시에 비용절감, 업무의 효율성, 서비스 품질 향상 등을 이유로 외부 기업 또는 개인사업자에게 개인정보 처리 업무를 위탁하여 수집된 개인정보를 수탁사에게 제공하고 있다. 이와 같이 기업의 개인정보 처리 업무 위탁 구조는 〔그림 1〕과 같이 표현될 수 있다.



〔그림 1〕 기업의 개인정보 처리 업무 위탁 구조

개인정보 처리 업무 위탁 즉, 수탁사가 증가할수록 제공되는 개인정보의 종류와 량이 증가하며 이에 따른 관리 포인트와 보안 위협도 함께 증가하게 된다.

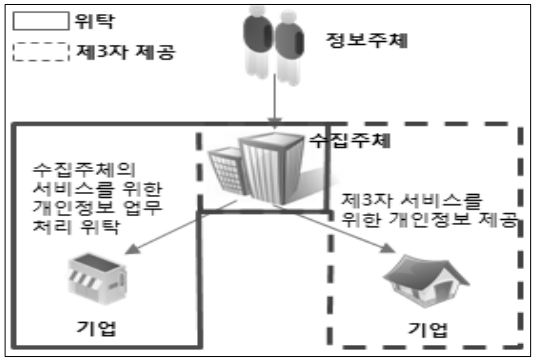
실제 보안사고를 살펴보면, A통신회사(위탁사)가 B회사(수탁사)에게 마케팅을 위한 고객관리 업무를 위탁하며 개인정보를 제공하였으나, B회사는 제공받은 개인정보를 정보주체에게 동의를 받지 않았으며 수집 목적 외로 제3자(C은행)에게 신용카드 발급 목적으로 제공한 사건이 발생하였다〔3〕. 또한, A택배업체(위탁사)가 B택배운송 개인사업자(수탁사)에게 배송업무 위탁을 위해 개인정보를 제공하였으나, B택배운송 개인사업자가 제공받은 개인정보를 유출하는 사건이 발생하였다.〔4〕

이와 같이 개인정보의 이용 및 제공이 빈번한 기업 구조에서는 수탁사에 의해 언제든지 개인정보가 유출될 수 있는 가능성이 존재한다. 또한, 법률에서는 개인정보 처리 업무 위탁에 대한 개인정보보호를 강화하기 위해 개인정보보호에 있어서 위탁사는 수탁사를 관리·감독해야 할 의무를 규정하고 있어 기업입장에서는 이를 위한 보안강화방법이 절실한 상황이다. 따라서, 본 연구에서는 개인정보 처리 업무 위탁에 대한 법률사항을 분석하고, 현재 개인정보 처리 업무를 위탁 받아 사업을 진행하는 수탁사들에 대한 개인정보보호 수준 분석 및 문제점을 도출하여 개인정보를 보호하고 수탁사들을 보다 효과적으로 관리·감독할 수 있는 방안에 대하여 제안하고자 한다.

II. 개인정보 처리업무 위탁의 개념 및 관련 법률

2.1 위탁과 제3자 제공

개인정보는 수집, 저장, 이용 및 제공, 파기의 라이프 싸이클이라는 흐름을 가지고 있다. 이 중에서 개인정보 제공의 의미는 "개인정보의 저장매체 또는 개인정보가 담긴 출력물이나 책자 등의 물리적 이전, 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전과 공동으로 이용할 수 있는 상태를 초래하는 모든 행위"를 뜻한다.〔5〕 즉, 정보주체로부터 수집한 개인정보를 정보주체와 수집주체 외의 제3자에게 이전, 전송, 공유, 접근허용 등의 포괄적인 행위로 해석할 수 있다.



〔그림 2〕 위탁과 제3자 제공의 구분

개인정보의 제공은 다시 개인정보의 처리업무 위탁과 제3자 제공으로 분류 될 수 있다. 정보주체로부터 수집된 개인정보가 제3자에게 이전, 제공, 공동이용되

는 측면에서 개인정보 처리업무 위탁과 개인정보의 제3자 제공은 동일하다고 할 수 있다. 하지만, '개인정보 처리업무 위탁'의 경우에는 수집주체(개인정보처리자)의 서비스 또는 업무를 처리할 목적으로 개인정보가 제3자(수탁자)에게 이전되는 것이며, '제3자 제공'은 그 제3자의 서비스 또는 업무를 처리할 목적 및 그 제3자의 이익을 위해서 개인정보가 이전 된다는 점이 다르다. 또한 업무위탁의 경우에는 개인정보가 이전된 후에도 개인정보처리자(수집주체)의 관리·감독을 받지만, 제3자 제공은 개인정보가 제공된 이후에는 제3자가 자신의 책임 하에 개인정보를 처리하게 되며 개인정보처리자(수집주체)의 관리·감독권이 미치지 못한다.[6] 위탁과 제3자 제공의 구분은 〔그림 2〕와 같이 표현될 수 있다.

판례를 살펴보면, 사건 내용은 〔표 1〕과 같다. 이 사건의 주요 쟁점 중 하나는 A사의 부가서비스 시행을 위한 개인정보 제공이 "제3자 제공"에 해당하는지 아니면 "위탁"에 해당하는지 여부이다. 이에 개인정보분쟁조정위원회는 ①당해 부가서비스가 통신사업자 본래의 통신서비스에 부수되어 시행된다는 점, ②제공된 개인정보는 당해 통신사업자의 부가서비스 제공에 한정되어 이용된다는 점, ③부가서비스는 당해 통신사업자의 고객에 한정하여 시행된다는 점, ④통신사업자의 "명의"로 부가서비스가 시행된다는 점을 고려해 볼 때, "개인정보처리 위탁"으로 봐야 할 것이라고 판단하였다.[7]

〔표 1〕 위탁과 제3자 제공의 구분 판례

사건 개요	○A사(초고속인터넷서비스 사업자)는 PC원격지원 부가서비스에 대한 위탁사실을 고지하지 않고 B사(부가서비스 업체)에 K씨의 개인정보를 제공함 ○A사의 웹사이트에는 "제휴업체가 부가 서비스를 제공한다"는 내용만 명시되어 있음 ○부가서비스에 가입하지 않은 K씨는 부가서비스 이용요금이 청구된 것을 확인하고 이에 대한 항의 중 A사와 B사가 별개의 회사임을 확인하고 본인의 동의 없이 제3자(B회사)에 개인정보를 제공한 것에 대해 제공 경위와 사과문을 요청함
A사 주장	○부가서비스에 관하여 자사의 이용약관 및 웹사이트에 관련 내용을 공지하고 있음(위탁)
K씨 주장	○A사와 B사는 엄연히 별개의 회사임에도 불구하고 이를 속이고 개인정보를 제공·이용한 행위는 개인정보를 침해임(제3자 제공)
분쟁조정 결정례	○PC원격지원 부가서비스는 개인정보 제공자(A사)의 사무처리를 위한 경우로 제3자 제공"이 아닌 "위탁"임 ○부가서비스를 위탁하는 경우 수탁자의 사업자명, 제공된 신청인의 개인정보 항목 등을 명확히 공개하는 것이 타당함

따라서, 기업이 개인정보 처리업무를 위탁할 시에는 업무의 성격을 명확히 파악하여 제3자 제공과 구분하여야 한다. 이는 개인정보 업무 처리 위탁과 제3자 제공에 대하여 개인정보보호법과 정보통신망법에서 요구하는 사항이 다르기 때문이기도 하다.

2.2 처리업무 위탁과 제3자 제공의 종류

개인정보 처리업무 위탁과 제3자 제공을 구분하기 위해서는 위탁사의 업무 또는 서비스의 연결성이 존재하는지 판단해야 한다. 예를 들어 콜센터 업무의 아웃소싱은 위탁사의 서비스에 대한 불만, 요청, 질문 사항 등을 처리하므로 개인정보 처리업무의 위탁이며, 물품 배송 업무는 위탁사가 판매하는 물품을 고객에게 배송하기 위해서 위탁사에서 처리해야 할 배송업무를 대행하는 것이므로 개인정보 처리업무의 위탁이라고 할 수 있다. 하지만, 통신회사가 타보험사의 TM활동을 위해 수집한 개인정보를 제공하는 것은 통신회사의 TM활동과 무관하게 보험사의 업무 또는 서비스를 위함이므로 제3자 제공이라고 할 수 있다. 또한, 기업이 직원정보를 항공사의 마일리지 통합 관리를 위해 제공하는 경우도 기업 업무 또는 서비스와 무관하게 항공사의 업무 영역인 마일리지 통합 관리를 위한 것이므로 제3자 제공이라고 할 수 있다. 이와 같은 처리업무 위탁과 제3제 제공에 따른 서비스 유형은 〔표 2〕와 같다.

〔표 2〕 처리업무 위탁과 제3자 제공의 서비스 유형

처리업무 위탁	제3자 제공
○콜센터 아웃소싱 ○대리점을 통한 개인정보 수집 ○요금고지서/DM/물품 발송 업무 ○A/S 아웃소싱 ○개인정보 수집 업무 ○채권추심 ○급여관리 ○직원채용 업무 ○청소관리 업무 ○주차관리 업무 ○전산시스템의 개발·관리·유지보수 업무 ○시스템 보안관리 업무 ○직원 교육 ○본인인증, I-PIN 인증 ○신용도 조회 ○카드결제, 가상계좌/무통장 입금 승인	○통신회사가 보험사 TM에 활용할 수 있도록 개인정보를 보험사에 제공 ○부가서비스 TM에 활용할 수 있도록 개인정보를 제휴사에 제공 ○호텔이 보험사와 공동으로 이벤트를 개최하여 응모한 개인정보를 카드 판촉에 이용되도록 카드회사에 제공 ○케이블방송사가 자회사인 초고속인터넷 업체의 TM에 활용하도록 고객정보를 자회사에 제공 ○기업이 직원정보를 항공사의 마일리지 통합 관리를 위해 항공사에 제공

2.3 관련 법률

2.3.1 개인정보보호를 위해 위탁사 및 수탁사가 지켜야 할 법률

개인정보보호법과 정보통신망법에서는 개인정보 처리업무 위탁 시 개인정보 라이프싸이클(수집, 저장, 이용 및 제공, 파기) 별로 위탁사가 준수해야 할 법률 사항을 명시하고 있다. 법에서 명시하고 있는 조항은 다음의 〔표 3〕과 같다.

〔표 3〕 위탁사가 준수해야 할 법 조항

구분	정보통신망법	개인정보보호법
수집	○ 제22조(개인정보의 수집·이용 동의 등) ○ 제27조의2(개인정보 취급방침의 공개) ○ 제24조의2(개인정보의 제공 동의 등)	○ 제22조(동의를 받는 방법) ○ 제30조(개인정보 처리방침의 수립 및 공개)
저장	○ 제28조(개인정보의 보호조치)	○ 제29조(안전조치의무)
이용 및 제공	○ 제24조(개인정보의 이용 제한) ○ 제25조(개인정보의 취급위탁) ○ 제30조(이용자의 권리 등) ○ 제30조의2(개인정보 이용내역의 통지)	○ 제17조(개인정보의 제공) ○ 제18조(개인정보의 이용·제공 제한) ○ 제26조(업무위탁에 따른 개인정보의 처리 제한) ○ 제35조(개인정보의 열람) ○ 제36조(개인정보의 정정·삭제) ○ 제37조(개인정보의 처리정지 등) ○ 제38조(권리행사의 방법 및 절차)
파기	○ 제29조 (개인정보의 파기)	○ 제21조 (개인정보의 파기)

개인정보의 수집에서는 정보통신망법 제27조의2와 개인정보보호법 제30조에 따라 개인정보취급방침(개인정보보호방침)에 개인정보처리의 위탁에 관한 사항을 명시해야 한다. 또한, 정보통신망법 제22조, 개인정보보호법 제22조에 따라 개인정보 수집 및 이용에 대하여 정보주체의 동의를 받아야 한다.

개인정보의 저장에서는 정보통신망법 제28조, 개인정보보호법 제29조에 따라 개인정보가 도난, 분식, 유출, 변조, 훼손되지 않도록 보호조치를 해야 한다.

개인정보의 이용 및 제공에서는 정보통신망법 및 개인정보보호법 모두 개인정보처리의 위탁에 대하여 제3자 제공과 구분하여 별도의 조항을 명시하고 있다. 따라서 기업은 정보통신망법 제25조에 따라 개인정보 업무 위탁 시 개인정보 수집 및 이용, 제3자 제공과 별도로 "개인정보 취급위탁을 받는 자", "개인정보 취급위탁을 하는 업무의 내용"에 대하여 동의를 받아야 한다. 하지만, 개인정보보호법에서는 "위탁하는 업무의 내용", "개인정보 처리 업무를 위탁받아 처리하는 자"에 대하여 공개만하면 된다. 또한, 두 법 모두 위탁사는 수탁사를 관리·감독할 위무를 부여하고 있으며, 수탁사가 개인정보를 유출하였거나 법률 위반 시 수탁사를 위탁사의 소속직원으로 간주하여 위탁사에도 손해배상책임을 부과하도록 규정하고 있다.

또한, 정보주체가 자신의 개인정보의 이용 및 제공 내역을 확인할 수 있는 법적 장치를 정보통신망법 제30조 및 개인정보보호법 제35조, 제36조, 제37조, 제38조에 명시하여, 위탁사는 언제든지 정보주체의 열람, 정정, 삭제, 처리정지 등의 요청에 대하여 수탁사에게 요구할 수 있으며, 정보주체가 이에 대한 결과를 확인할 수 있는 방법을 제공해야 한다. 특히, 정보통신망법 제30조의2에서는 정보주체에게 년 1회이상 개인정보의 이용내역을 통지하도록 명시(2012년 2월 17일 신설)하고 있어 기업이 개인정보 업무처리를 위해 제공한 개인정보에 대하여 이전보다 강화된 관리의무를 부여하고 있다.

개인정보 파기에서는 정보통신망법 제29조 및 개인정보보호법 제21조에 따라 정보주체의 삭제 요구, 개인정보 보유기간 경과, 처리 목적 달성 시 기업에 보관되어 있는 개인정보 뿐만 아니라 수탁사에 제공한 개인정보도 함께 파기해야 한다.

이처럼 법률에서는 개인정보 처리업무 위탁에 있어서 개인정보를 처리하는 주체가 수탁사일지라도 개인정보의 수집 주체는 위탁사(기업)이고 위탁사의 서비스를 위해 제공하였으므로 수탁사의 관리·감독 및 개인정보유출 사고에 대하여 책임과 의무를 부여하고 있는 것이다.

한편, 수탁사가 준수해야 할 법조항은 개인정보보호법 제26조 제5항, 제7항 및 정보통신망법 제67조 제5항에 명시되어 있으며, 수탁사도 개인정보의 수집, 저장, 이용 및 제공, 파기의 개인정보 라이프 싸이클 전반에 대하여 위탁사와 동일한 수준으로 개인정보를 보호해야 할 의무를 부여하고 있다.

개인정보보호법과 정보통신망법에서 수탁사가 준수해야 할 법 조항을 정리하면 〔표 4〕와 같다.

〔표 4〕 수탁사가 준수해야 할 법 조항

정보통신망법	개인정보보호법
제67조(방송사업자에 대한 준용) ② 제25조제1항에 따른 수탁자에 관하여는 제22조, 제23조, 제23조의2부터 제23조의4까지, 제24조, 제24조의2, 제26조, 제26조의2, 제27조, 제27조의2, 제27조의3, 제28조, 제28조의2, 제29조, 제30조, 제30조의2 및 제31조를 준용한다.	제26조(업무위탁에 따른 개인정보의 처리 제한) ⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다. ⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

III. 수탁사 개인정보보호 실태분석

3.1 개인정보보호 수준 분석 방법

개인정보보호를 위한 기업의 수탁사 관리 실태를 조사하기 위해 우선적으로 수탁사들의 개인정보보호 수준평가를 실시하였다. 수탁사들에 대한 수준평가 방법은 자기기입식 설문조사 방식을 채택하였다. 또한, 이 방식의 단점을 보완하기 위해 각 점검항목에 대한 증빙자료 제출을 요구하고 이를 분석 후 실사를 통해 사실 유무를 확인하여 신뢰성을 높였다. 점검항목은 정보통신망법 및 개인정보보호법을 기준으로 법적 준거성 확보에 중점을 두어 제작하였으며 구성은 다음 〔표 5〕와 같다.

〔표 5〕 수탁사 개인정보보호 수준평가 점검내용

도메인	점검내용	법적근거	
		정보통신망법	개인정보보호법
1.개인정보 보호 내부 관리계획 및 개인정보취급방침 수립	개인정보관리책임자지정 및 위탁사 통보, 개인정보보호 내부관리계획 및 개인정보취급방침 수립	제27조, 제27조2, 제28조	제29조, 제30조, 제31조
2.개인정보 취급자 관리	개인정보 취급 처리 현황 관리, 교육, 보안서약서 작성	기술적 보호조치 제3조1항, 2항, 3항	안전성 확보조치 제3조 1항, 2항
3.개인정보 수집	개인정보 수집 항목	제23조, 제23조의2	제16조
4.개인정보 저장 및 관리	개인정보 암호화 및 문서관리	기술적 보호조치 제6조	안전성 확보조치 제7조, 제10조
5.개인정보 처리	개인정보 처리 기록 관리, 출력 및 복사 관리	기술적 보호조치 제5조, 제8조	안전성확보조치 제8조
6.개인정보 제공	개인정보 재위탁 및 제3자 제공	제25조 1,2항	제18조, 19조
7.개인정보 파기	개인정보 파기 관리, 파기 내용 위탁사에 통보	제29조	제21조
8.개인정보 처리 시스템의 보호조치	개인정보취급자 접속기록 위·변조 방지, 개인정보취급자 계정 이력 관리, 개인정보취급자 접근권한 변경 관리, 접근통제 장치 설치 유무	기술적 보호조치 제4조, 5조	안전성 확보조치 제4조, 제6조, 제8조
9.개인정보 열람/정정/삭제 요구 대응	개인정보 열람/정정/삭제/정지 요구 대응 조치	제30조	제35조, 제36조, 제37, 제38조

보안수준 평가방법은 각 점검항목에 대한 중요도를 〔표 6〕과 같이 법률에 명시되어 있으며 법률 미준수 시 과태료가 부과되는 항목은 H(3점), 단순 법률 명시항목은 M(2점), 법률에 명시되어 있지 않으며 과태료도 없는 항목은 L(1점)으로 구분하였으며, 점검결과는 〔표 7〕과 같이 완료는 Y(1점), 부분완료는 P(0.5점), 미완료 또는 해당사항이 없으면 N 또는 N/A(0점)으로 평가하여 각 점검항목별 평가결과, 도메인별 전체점수, 전체 보안수준으로 산출하였다. 보안수준 산출식은 〔표 8〕과 같다.

〔표 6〕 중요도 평가 기준 및 점수

중요도	점수	중요도 기준
H	3	법률 명시 및 과태료
M	2	법률 명시
L	1	해당 없는 항목

〔표 7〕 점검결과에 따른 점수

점검결과	점수
Y	1
P	0.5
N or N/A	0

〔표 8〕 보안수준 산출식

보안수준 산출식
○각 항목별 평가결과 = 중요도 X 점검결과 ○도메인별 전체점수 = N/A를 제외한 중요도 점수의 합 ○도메인별 평가점수 = N/A를 제외한 각 항목별 평가결과의 합 ○도메인별 보안수준(%) = (도메인별 평가점수)/(도메인별 전체점수) ○총 평가점수 = 도메일별 평가점수의 합 ○총 보안수준(%) = (도메인별 평가점수의 합)/(도메인별 전체점수의 합)

설문조사는 2012년 1월부터 4월까지 4개 기업에서 개인정보 처리 업무 위탁을 받은 총 65개 수탁사를 대상으로 진행되었으며, 65개(100%) 수탁사의 설문 및 증빙자료가 회수되었다.

3.2 개인정보보호 수준 일반 현황

총65개 수탁사를 위탁업무 특성에 따라 실명인증 및 추심업무 위탁업체(9개), DM 발송 위탁업체(10개), SMS/MMS 발송 위탁업체(4개), 카드/매거진 배송위탁업체(8개), 상품배송 위탁업체(8개), 개인영상정보(CCTV) 시스템 유지보수 위탁업체(3개), 상품API 개발 위탁업체(6개), 기타 업무 위탁업체(6개), 콜센터 위탁업체(6개) 등 총 9개의 위탁업무 군으로 분류하였다.

위탁업무별 평균 보안수준은 〔표 9〕와 같이 45.7%로 낮은 수준인 것으로 조사되었다. SMS/MMS 발송 위탁업체가 78.8%로 가장 높은 보안수준 및 법적 준거성을 만족하였으나, 그 외의 위탁군은 50%를 조금 상위하거나 그 이하로 조사되어 수탁사를 통한 개인정보 유출사고의 발생 가능성이 높은 것으로 확인되었다.

〔표 9〕 위탁업무별 보안수준

위탁업무	보안수준
실명인증, 추심업무	50.2%
DM 발송	52.6%
SMS/MMS 발송	78.8%
카드/매거진 발송	41.8%
상품 배송	37.1%
개인영상정보 시스템 유지보수	20.5%
기타 업무 (보증보험발급대행, 소액결제, 보험처리)	53.3%
상품API 개발	33.5%
콜센터	43.3%
평균	45.7%

점검 도메인별 평균 보안수준은 〔표 10〕과 같이 45.5%로 낮은 수준인 것으로 조사되었다. 각 도메인별로 살펴보면, 개인정보 제공 부분은 90.0%로 높은 보안수준을 나타냈지만 개인정보보호 내부관리계획 및 개인정보취급방침 수립, 개인정보 취급자 관리, 개인정보 라이프싸이클(수집은 최소정보 수집에 대한 적합성만 판단함) 등 전반적인 부분에서 50%이하로 낮은 보안수준을 나타내고 있어 이에 대한 대책 마련이 시급하다고 할 수 있다.

〔표 10〕 점검 도메인별 보안수준

점검 도메인	보안수준
개인정보보호 내부관리계획 및 개인정보취급방침 수립	48.2%
개인정보 취급자 관리	46.5%
개인정보 수집	N/A
개인정보 저장 및 관리	49.2%
개인정보 처리	46.6%
개인정보 제공	90.0%
개인정보 파기	32.9%
개인정보처리시스템의 보호조치	44.2%
개인정보 열람/정정/삭제 요구 대응	33.1%
평균	45.5%

3.3 개인정보보호 수준 분석 세부 결과

3.3.1 개인정보보호 내부관리계획 및 개인정보취급방침 수립

수탁사들의 개인정보보호 내부관리계획 및 개인정보취급방침 수립에 대한 보안수준은 48.2%로 조사되었다. 수탁사의 32.3%(21개)가 자체적인 개인정보보호 내부관리계획 수립하고 있으며, 40.0%(26개)가 개인정보취급방침을 보유하고 있는 것으로 조사되었다. 이는 개인정보를 수집하는 일반 사업체의 53%〔8〕에 비해 낮은 수치이다.

또한, 개인정보관리책임자가 지정되어 있고 이를 위탁사에 통보하는 수탁사는 47.7%(31개)인 것으로 조사되었다. 특히, 개인정보관리책임자가 지정되어 있으며, 개인정보보호 내부관리계획과 개인정보취급방침이 수립되어 있는 수탁사는 30.8%(20개)에 불과한 것으로 조사되었다. 개인정보관리책임자가 지정되어 있으나 개인정보보호 내부관리계획 및 개인정보취급방침이 수립되어 있지 않다는 것은 개인정보관리책임자가 개인정보보호의 관리·감독 의무를 다하지 않고 있다는 것이다. 반대로 개인정보보호 내부관리계획 및

〔표 11〕 개인정보보호 내부관리계획 및 개인정보취급방침 수립 보안수준

점검항목	중요도	Y (빈도율)	N (빈도율)	P (빈도율)
개인정보관리책임자 지정 및 위탁사 통보 여부	H	31 (47.7%)	28 (43.1%)	6 (9.2%)
개인정보보호 내부관리계획 수립 여부	H	21 (32.3%)	30 (46.2%)	14 (21.5%)
개인정보취급방침 보유 여부	H	26 (40.0%)	27 (41.5%)	12 (18.5%)
전체점수		585점		
평가점수		282점		
보안수준		48.2%		

개인정보취급방침이 수립되어 있으나 개인정보관리책임자가 지정되어 있지 않다는 것은 책임자 부재로 인하여 개인정보보호의 체계적인 관리가 어려울 것이며, 개인정보 처리민원 및 유출사고 발생 시 신속하게 대처할 수 없을 것이다.

3.3.2 개인정보취급자 관리

수탁사들의 개인정보취급자 관리에 대한 보안수준은 46.5%로 조사되었다. 이 중 개인정보취급자에 대한 현황을 관리하고 있는 곳은 41.5%(27개), 개인정보취급자에 대하여 년2회 이상 교육을 진행하고 있는 곳은 12.3%(8개), 개인정보취급자 채용 시 보안서약서를 징구하고 있는 곳은 66.2%(43개)로 확인되었다.

특히, 개인정보취급자 현황 관리는 기업내부에서 부서이동, 전배, 퇴사, 입사 등에 의해 개인정보취급자 계정의 권한변경이 발생할 경우 이를 체계적으로 관리하여 비인가자로부터 개인정보를 보호해야 하기 때문에 특별한 관리가 필요하다. 또한, 개인정보취급자에 대한 교육을 실시하지 않는 수탁사가 76.9%(50개), 년1회만 실시하는 수탁사가 10.8%(7개)로 조사되어 주기적인 교육을 통해 개인정보보호 및 보안 인식 수준을 높이고 법률 준수사항을 인지시킬 필요가 있다.

〔표 12〕 개인정보취급자 관리 보안수준

점검항목	중요도	Y (빈도율)	N (빈도율)	P (빈도율)
개인정보취급자 현황 관리	H	27 (41.5%)	31 (47.7%)	7 (10.8%)
개인정보취급자에 대한 교육 여부(년2회)	H	8 (12.3%)	50 (76.9%)	7 (10.8%)
개인정보취급자 채용 시 보안서약서 작성 여부	H	43 (66.2%)	11 (16.9%)	11 (16.9%)
전체점수		455점		
평가점수		211.5점		
보안수준		46.5%		

3.3.3 개인정보 수집

개인정보 수집에 대한 보안 수준은 위탁업무별로 개인정보 처리업무 목적에 필요한 최소 정보만을 수집하는지에 대한 적합성을 점검하였다. 〔표 13〕과 같이 대부분의 수탁사가 개인정보처리업무에 필요한 최소한의 개인정보만을 제공받고 있으나, 상품API개발 수

〔표 13〕 위탁업무별 개인정보 수집 항목

위탁업무	수집 항목	처리목적	적합성
실명인증, 추심업무	이름, 주민등록번호, 주소, 자택번호, 휴대폰번호, 직장주소, 성별, 이메일	본인확인 및 채권추심	적합
DM 발송	이름, 주소, 자택번호, 휴대폰번호, 직장주소, 직장전화번호, 성별, 결혼유무, 기념일	DM 및 안내문 배송	적합
SMS/MMS 발송	이름, 휴대폰번호	SMS 안내	적합
카드/매거진 발송	이름, 주소, 자택번호, 휴대폰번호, 직장번호, 직장주소	카드 및 매거진 배송	적합
상품 배송	이름, 이메일, 주소, 자택번호, 휴대폰번호, 직장전화번호, 직장주소	구매물품 배송 처리	적합
개인영상정보 시스템 유지보수	이름, 주소, 휴대폰번호, 이메일	영상정보 시스템 유지 보수	적합
기타 업무(보증보험발급대행, 소액결제, 보험처리)	이름, 주민등록번호, 이메일, 주소, 카드번호, 계좌번호, 자택번호, 휴대폰번호, 직장전화번호, 직장주소	보증보험 증서 발급, 소액결제	적합
상품API 개발	주민등록번호, 이름, 신용카드번호, 계좌번호, 이메일, 주소, 자택번호, 휴대폰번호, 직장주소	개발 유지 보수	부적합
콜센터	이름, 이메일, 주소, 자택전화번호, 휴대폰번호, 직장전화번호, 직장주소, 성별	민원 응대	적합

탁업체의 경우 개발 시 주민등록번호를 제공받고 있어 정보통신망법 제23조의2(주민등록번호의 사용 제한)에 의거 향후 삭제할 필요가 있다.

3.3.4 개인정보 저장 및 관리

수탁사들의 개인정보 저장 및 관리에 대한 보안수준은 49.2%로 조사되었다.

〔표 14〕 개인정보 저장 및 관리 보안수준

점검항목	중요도	Y (빈도율)	N (빈도율)	P (빈도율)
개인정보의 저장 및 전송 시 암호화 여부	H	34 (52.3%)	19 (29.2%)	11 (16.9%)
개인정보가 포함된 문서를 보안장치가 설치된 장소에 보관하고 있으며, 문서 이관 시에 보안 절차 시행 여부	H	8 (12.3%)	25 (38.5%)	31 (47.7%)
전체점수		384점		
평가점수		189점		
보안수준		49.2%		

개인정보의 저장 및 전송 시 암호화를 적용하고 있는 수탁사는 52.3%(34개)로 조사되었으며, 저장 시에만 암호화를 적용한 수탁사가 16.9%(11개)사로 조사되어 개인정보 암호화에 대한 적용이 시급하다. 또한, 개인정보가 포함된 문서 보관 시 보안장치가 설치된 안전한 장소에 보관하는 수탁사는 12.3%(8개)로 매우 낮게 조사되었으며, 수탁사의 87.7%(56개)가 계약서는 보안장치가 설치된 캐비넷이나 문서보관함에 보관하고 있었으나 개인정보가 포함된 일반 문서는 방치하고 있어 문서를 통한 개인정보 유출 가능성이 존재하였다.

3.3.5 개인정보 처리

수탁사들의 개인정보 처리에 대한 보안수준은 46.6%로 조사되었다. 개인정보처리시스템 즉, DBMS에 대한 개인정보취급자의 접근내역을 저장하고 있는 수탁사는 49.2%(32개)로 낮은 준수율을 보이고 있으며, 16.9%(11개)는 부분적으로 적용하고 있는 것으로 조사되었다. 또한, 개인정보가 기록되어 있는 문서에 대한 출력 및 복사 시 이에 대한 개인정보관리책임자의 승인을 받고 관리대장을 기록·관리하고 있는 수탁사는 41.5%(27개), 관리대장만 기록하고 있는 수탁사가 9.2%(6개)로 조사되었다. 따라서, 개인정보 유출 사고 발생 시 책임추적에 어려움이 존재하여 이에 따른 보안이 시급하다.

〔표 15〕 개인정보 처리 보안수준

점검항목	중요도	Y (빈도율)	N (빈도율)	P (빈도율)
개인정보처리시스템 접근내역 저장 유무	H	32 (49.2%)	22 (33.8%)	11 (16.9%)
개인정보의 출력/복사 시에 출입/복사 관리 대장 기록 및 개인정보관리책임자의 승인 유무	H	27 (41.5%)	32 (49.2%)	6 (9.2%)
전체점수		325점		
평가점수		151.5점		
보안수준		46.6%		

3.3.6 개인정보 제공

수탁사들의 개인정보 제공에 대한 보안수준은 90.0%로 조사되었다. 수탁사의 20.0%(13개)가 개인정보 처리업무 위탁계약서에 〔표 16〕과 같이 재위탁 및 제3자 제공 금지조항이 존재하지 않는 것으로 확인 되었다.

〔표 16〕 개인정보 처리업무 위탁계약서 내용

항목	내용
목적	○계약 목적
업무목적 외 사용 금지	○업무목적 외 사용 금지
개인정보의 활용 제한	○업무목적 외 별도 저장, 출력 금지
이용자 관리	○개인정보 관리 책임자 지정 및 취급자 지정
정보의 송수신	○개인정보 송수신 시 암호화
개인정보의 폐기 및 반납	○목적 및 보존기간 만료 시 폐기
책임 및 손해배상	○개인정보 유출 시 손해배상 청구
효력발생 및 유효기간	○본 계약서의 효력 및 유효 기간 정의
교육	○정기적인 정보보호 교육
기타	○기타 내용

따라서, 수탁사의 무분별한 재위탁, 제3자 제공과 이로 인한 개인정보 유출 사고 발생 시 법적책임을 부

〔표 17〕 개인정보 제공 보안수준

점검항목	중요도	Y (빈도율)	N (빈도율)	P (빈도율)
위탁사로 부터 제공받은 개인정보의 재위탁 또는 제3자 제공 여부	H	52 (80.0%)	0 (0%)	13 (20.0%)
전체점수		130점		
평가점수		117점		
보안수준		90.0%		

과하기 어려운 상황이 발생할 수 있으므로 “개인정보의 재위탁 및 제3자 제공 금지” 항목을 추가한 계약서의 갱신이 시급하다.

3.3.7 개인정보 파기

수탁사들의 개인정보 파기에 대한 보안수준은 32.9%로 조사되었다. 개인정보 이용 목적 달성 후 지체 없이 파기하고 그 결과를 위탁사에 통보하는 수탁사는 10.8%(7개)로 매우 낮은 준수율을 나타내고 있다. 수탁사 중 40.0%(26개)는 목적이 달성된 개인정보에 대하여 지체 없이 파기를 하고 있으나 파기 결과를 위탁사에 통보하지 않고 있어 위탁사는 이에 대한 철저한 관리가 필요하다. 또한, 개인정보 파기 시 파일완전삭제 프로그램 및 장치 완전파괴 방법을 사용하고 있는 수탁사는 30.8%(20개)로 조사되었으며, 두 방법 중 하나만 사용하고 있는 수탁사가 10.8%(7개), 완전삭제 및 파괴 방법을 사용하지 않는 수탁사가 24.6%(16)개로 조사되어 하드 또는 외부 저장장치가 유출 되었을 시 파일을 복구를 통해 개인정보가 유출될 가능성이 존재하는 것으로 나타났다.

〔표 18〕 개인정보 파기 보안수준

점검항목	중요도	Y (빈도율)	N (빈도율)	P (빈도율)
개인정보(문서, 데이터 파일 형태)의 이용목적 달성 후 개인정보파기 규정에 따른 지체 없이 파기와 파기결과에 대한 위탁사 통보 여부	H	7 (10.8%)	32 (49.2%)	26 (40.0%)
개인정보파일 삭제 시 파일완전삭제 프로그램의 사용 여부 및 장치폐기 시 물리적 완전파괴 방법 사용 여부	H	20 (30.8%)	38 (58.5%)	7 (10.8%)
전체점수		325점		
평가점수		107점		
보안수준		32.9%		

3.3.8 개인정보처리시스템 보호조치

수탁사들의 개인정보처리시스템 보호조치에 대한 보안수준은 44.2%로 조사되었다. 개인정보취급자의 접속기록에 대한 백업을 수행하지 않는 수탁사가 23.1%(15개)이며 부분적으로 시행하고 있는 수탁사 41.5%(27개)로 조사되어 수탁사의 절반 이상이 접속기록 위/변조 방지에 대한 대책이 부재한 것으로 나타났다. 개인정보처리시스템 및 업무용PC에 접근통제 장치가 미설치된 수탁사가 46.2%(30개)이며 부분적으로 적용된 수탁사가 21.5%(14개)로 매우 낮은 수준으로 조사되어 비인가자의 의한 개인정보 유출 가능성이 높은 것으로 조사되었다. 또한, 개인정보취급자의 인사이동 및 퇴직 시 접근권한에 대한 변경, 말소처리 여부는 부분적으로 시행하고 있는 수탁사가 53.8%(14개)이며 시행하고 있지 않은 수탁사가 21.5%(14개)로 조사되었다. 이와 함께 개인정보취급자의 인사이동에 따른 접근권한 변경처리에 대하여 부분적용하고 있는 수탁사가 53.8%(35개)이며 적용하고 있지 않는 수탁사가 21.5%(14개)로 조사되었다. 이 두 항목에 대해서는 전체 수탁사 중 75%이상이 법률을 준수하지 않고 있어 악의적인 내부 사용자에 의해 계정정보가 탈취되었을 시 개인정보 유출 가능성이 존재하여 시급한 보안조치가 필요하다

〔표 19〕 개인정보처리시스템 보호조치 보안수준

점검항목	중요도	Y (빈도율)	N (빈도율)	P (빈도율)
개인정보취급자의 접속기록 위/변조 방지를 위한 정기적인 백업 수행 여부	H	23 (35.4%)	15 (23.1%)	27 (41.5%)
개인정보처리시스템 계정 또는 업무용PC사용자 이력 관리 여부	H	8 (12.3%)	46 (70.8%)	11 (16.9%)
개인정보취급자의 인사이동 및 퇴직 시 접근권한 변경 및 말소처리 여부	H	16 (24.6%)	14 (21.5%)	35 (53.8%)
개인정보처리시스템 및 업무용PC에 대한 접근통제 장치 설치 여부	H	21 (32.3%)	30 (46.2%)	14 (21.5%)
전체점수		650점		
평가점수		287.5점		
보안수준		44.2%		

3.3.9 개인정보 열람/정정/삭제 요구 대응

수탁사의 개인정보 열람/정정/삭제 요구 대응에 대한 보안수준은 33.1%로 조사되었다. 정보주체가 자신의 개인정보에 대한 열람/정정/삭제/처리정지 요구에 대하여 내부적인 처리절차가 마련되어 있지 않은 수탁사가 66.2%(43개)로 나타났으며 부분적으로 마련되어 있는 수탁사가 1.5%(1개)로 조사되었다. 따라서, 정보주체가 위탁사 또는 수탁사에게 자신의 개인정보에 대한 열람/정정/삭제/처리정지 요구 시 체계적인 대응이 어려워 정보주체 및 위탁사와의 분쟁이 발생할 가능성이 높은 것으로 나타났다.

〔표 20〕 개인정보 열람/정정/삭제 요구 대응 보안수준

점검항목	중요도	Y (빈도율)	N (빈도율)	P (빈도율)
정보주체가 자신의 개인정보에 대한 열람/정정/삭제 등의 요구 시 조치절차 수립 여부	H	21 (32.3%)	43 (66.2%)	1 (1.5%)
정보주체가 자신의 개인정보의 이용 및 처리정지 요구 시 이에 대한 조치절차 수립 여부	H	21 (32.3%)	43 (66.2%)	1 (1.5%)
전체점수		390점		
평가점수		129점		
보안수준		33.1%		

IV. 개인정보보호를 위한 수탁사 관리 방안

4.1 개인정보보호를 위한 수탁사 관리체계 수립

조사된 수탁사의 개인정보보호 수준평가를 바탕으로 기업의 개인정보보호를 위한 수탁사 관리체계 강화 방안을 살펴보면 다음과 같다.

첫째, 수탁사의 개인정보보호 내부관리계획 수립을 위한 표준양식 및 위탁업무 표준 계약서가 마련되어야 한다. 실태점검 결과를 통해 알 수 있듯이 수탁사 중 30.8(20개)%만이 개인정보보호 내부관리계획 및 개인정보취급방침을 수립하고 있어 이에 대한 보안이 시급하다. 수탁사가 자체적으로 개인정보관리책임자를 지정하고 개인정보보호 내부관리계획 및 개인정보취급방침을 수립해야 하지만 위탁사의 수탁사 관리·감독 의무와 책임 관점에서 봤을 때 위탁사는 제공된 개인정보를 보호하고 수탁사들을 효율적으로 관리하기 위한 개인정보보호 내부관리계획 표준양식을 제공하여 수탁사로 하여금 이를 따르게 할 필요성이 있다. 개인정보보호 내부관리계획 표준양식 내용은 〔표 21〕과 같다.

〔표 21〕 개인정보보호 내부관리계획 표준양식 내용

항목	내용
총칙	○목적 ○적용범위 ○용어 정의
내부관리계획의 수립 및 시행	○내부관리계획의 수립 및 승인 ○내부관리계획의 공표
개인정보관리책임자의 의무와 책임	○개인정보관리책임자의 지정 ○개인정보관리책임자의 의무와 책임 ○개인정보취급자의 법위 및 의무와 책임
개인정보 수집 이용 시 처리절차	○개인정보의 수집 ○개인정보의 이용 및 제공의 제한
개인정보취급방침 수립	○개인정보의 수집이용 목적 ○수집하는 개인정보항목 및 수집방법 ○개인정보의 처리 및 보유기간 ○개인정보의 제3자 제공 ○개인정보의 위탁 ○정보주체의 권리·의무 및 그 행사방법에 관한 사항 ○이용자 및 법정대리인의 권리와 그 행사방법 ○개인정보의 파기절차 및 방법 ○개인정보관리책임자의 성명, 부서, 연락처
개인정보의 기술적·관리적 보호조치	○출력 복사 시 보호조치 ○개인정보취급자 접근권한관리, 인증 ○개인정보의 암호화 ○접근통제 ○접속 기록의 위변조 방지 ○보안프로그램의 설치 및 운영 ○물리적 접근제한
정기적인 자체감사	○자체감사 주기 및 절차 ○자체검사 결과 반영
개인정보보호 교육	○개인정보보호 교육 계획의 수립 ○개인정보보호 교육의 실시
개인정보 침해대응 및 피해구제	○개인정보 침해대응 절차 ○피해구제 방안

또한, 위탁사는 개인정보 처리업무 위탁에 대한 계약 시 〔표 22〕와 같은 내용이 포함된 일괄된 표준 계약서를 적용하여 수탁사 스스로가 제공받은 개인정보를 보호하도록 유도하고 수탁사에 대한 개인정보보호 실태점검을 강제화해야 할 필요가 있다. 표준 위탁 계약서는 안행부에서 제공하는 "표준 개인정보처리위탁 계약서(안)"을 참고하였으며 개인정보취급방침 수립, 개인정보관리책임자 지정, 보안점검 리스트 항목, 개

〔표 22〕 표준 위탁 계약서 내용

항목	내용	비고
목적	○계약서 목적	
위탁 업무 수행 목적 외 개인정보 처리 금지	○정보주체의 동의가 없거나 목적 외의 개인정보 처리 금지	
위탁업무의 목적 및 범위	○위탁 업무 목적과 그 범위 정의	
재위탁 제한	○위탁사와 협의 없는 재위탁 금지	
개인정보의 기술적·관리적·물리적 보호조치	○내부관리계획 수립	
	○개인정보취급방침 수립	추가
	○개인정보관리책임자 지정	추가
	○그 밖의 개인정보보호를 위한 기술적/관리적 보호조치 사항	
수탁사에 대한 관리·감독 및 교육	○개인정보보호를 위한 수탁사 보안점검 의무화	
	○보안점검 리스트	추가
	○개인정보보호 교육(년2회 이상) 의무화	추가
	○보안점검 결과에 따른 제재 및 계약 파기	추가
손해배상	○개인정보 유출 시 손해배상 청구	
효력발생 및 유효기간	○본 계약서의 효력 및 유효 기간 정의	추가

인정보보호 교육 의무화, 보안점검 결과에 따른 제재 및 계약 파기, 계약서의 효력 및 유효 기간을 추가하였다.

둘째, 수탁사의 개인정보 취급자를 대상으로 주기적인 개인정보보호 및 정보보호 교육이 필요하다. 위탁사는 개인정보보호법의 개인정보 안전성 확보조치 기준 제3조 2항 및 정보통신망법 안정성확보조치 제3조 4항에 의거하여 개인정보취급자에 대한 주기적인 교육을 실시해야 한다. 교육방법으로는 집체교육, 온라인 교육, 세미나 참석 등의 방법이 있을 것이며, 이에 대한 증적자료(온라인 교육 수료 결과, 세미나 참석증)를 요구하여 교육 참석 유무를 확인할 필요가 있다. 〔표 23〕의 교육내용과 같이 개인정보 수집, 저장, 활용, 파기 시 주의사항 및 개인정보 기술적 관리적 보호조치 등에 대한 교육을 통해 법적 의무와 책임을 인지시켜야 한다. 또한, 실제 개인정보가 유출되는 경로, 책임소지, 피해보상, 소송 내용을 반영한 개인정보 유출 사고 예시 등을 통해 개인정보취급자 스스로가 개인정보를 처리함에 있어서 경각심을 느낄 수 있

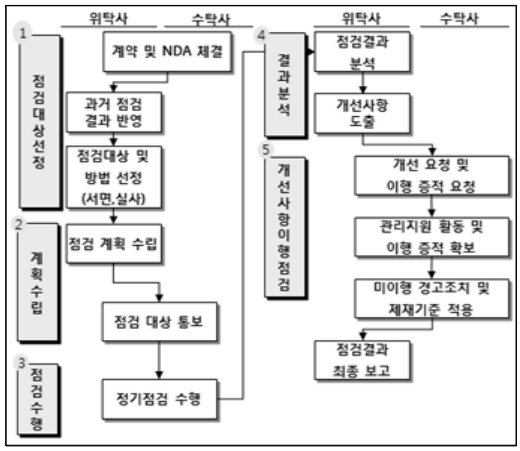
〔표 23〕 교육 내용

교육대상	수탁사의 개인정보취급자
교육시기/방법	○시기 : 연 2회 ○방법 : 집체교육
업무 특성에 따른 교육내용	○개인정보 처리 업무 위탁 시 의무 조치사항 (개인정보 생명주기 관련) - 수집 위탁 시 주의사항 - 개인정보 저장 시 주의사항 - 개인정보 활용 시 주의사항 - 개인정보 파기 시 주의사항 ○접근통제장치 관리, 출력/복사 관리 등 보호조치 관련 사항
공통 교육내용	○개인정보보호 관련 법률(정보통신망법, 개인정보보호법 등) ○개인정보 유출 사고 발생 시 책임 소재 및 피해보상 소송 내역 등 ○계약서 및 보안관리 약정서 내 개인정보보호 의무 ○개인정보 관리 수준 진단 서면 작성 방법 ○수탁사 업무자 준수 수칙

도록 해야 한다.

셋째, 수탁사에 대한 개인정보보호 실태점검 프로세스가 수립되어야 한다. 수탁사 개인정보보호 실태점검 프로세스는 〔그림 3〕과 같이 "수탁사 점검대상 선정", "실태점검 계획 수립", "수탁사 점검 수행", "점검결과 분석", "개선사항 이행점검"의 총 5단계로 구성된다.

"수탁사 점검대상 선정" 단계는 기존 점검결과를 반영하여 법적 준수율에 따라 현장점검 및 서면점검 대상을 선정한다. 만약, 신규계약 또는 업무 변경 시 라면 현장점검 수행을 실시한다. "실태점검 계획 수립"단계는 연간 점검계획 수립하고 점검 대상이 되는 수탁



〔그림 3〕 수탁사 개인정보보호 실태조사 프로세스

사들에게 점검계획을 통보한다. “수탁사 점검 수행” 단계는 서면점검, 담당자 인터뷰 및 현장 실사를 통해 수탁사의 개인정보보호 실태점검을 수행한다. “점검결과 분석” 단계는 수탁사들에 대한 개인정보보호 실태점검결과 분석을 통해 개인정보 관리현황을 파악하고 이에 대한 개선사항을 도출 후 점검결과를 통보한다. “개선사항 이행점검” 단계는 수탁사들의 개선사항 조치내역에 대하여 주기적 모니터링을 실시 후 개선사항 미 조치 시 제재기준을 적용한다. 위탁사는 이와 같은 5단계의 개인정보보호 실태점검 프로세스를 통해 주기적으로 수탁사를 점검하고 개인정보보호 수준을 파악하여 법적 준거성 확보 및 수탁사를 통한 개인정보 유출 사고를 방지해야 한다.

넷째, 수탁사 관리·감독 및 통제를 위한 기준이 마련되어야 한다. 위탁사는 수탁사 개인정보보호 실태점검 프로세스를 통해 법 준수율 및 보안수준을 파악했다면 그 결과에 따라 수탁사를 통제할 수 있는 기준을 마련해야 한다. 수탁사 개인정보보호 실태점검 결과를 바탕으로 〔표 24〕의 관리 기준에 따라 미이행 사항에 대하여 벌점을 부과한다. 벌점 기준은 법률 위반 시 과태료 대상 항목은 각1점, 징역 대상 항목은 각9점으로 적용하였다. 총 벌점을 산출하여 〔표 25〕의 벌점

〔표 24〕 위반 시 벌점 기준

관리 기준(준수 사항)	벌점	기준
개인정보보호 내부관리계획 미수립	1점	법률 위반 시 과태료
개인정보취급방침 미수립	1점	
개인정보관리책임자 미선임 및 미통보	1점	
개인정보 취급자 현황 미관리	1점	
개인정보 취급자 교육 미실시	1점	
정보보호 서약서 미징구	1점	
위탁서비스와 무관한 개인정보 수집	1점	
개인정보 암호화 미조치	1점	
개인정보 포함 문서에 대한 보안 미조치	1점	
개인정보처리시스템 접속기록 미저장	1점	
출력물 관리대장 미관리	1점	
개인정보 미파기	1점	
개인정보파기 시 완전삭제 미적용	1점	
접속기록 백업 미실시	1점	
개인정보처리시스템 및 업무PC 계정 이력 미관리	1점	
개인정보취급자 계정 이력 미관리	1점	
접근통제 미적용	1점	
개인정보 열람/정정/삭제 요구 미대응	1점	
개인정보 이용/처리정지 요구 미대응	1점	
개인정보 유출 사고	9점	법률 위반 시 징역
위탁사와 협의 없는 제3자 제공 및 재위탁	9점	

〔표 25〕 벌점별 제재 기준

총 벌점	제재 사항	보안수준
유출사고 발생	위탁계약 해지 및 손해배상 청구	-
9점 이상	위탁계약 해지	50%이하
5~8점	경고	51%~79%
1~4점	주의	80%이상
0점	없음	100%

별 제재 기준을 적용하고 다수의 위반 활동 적발 시 손해배상 청구 및 위탁계약을 해지하거나 차기 계약 시 불이익 반영 등의 강력한 조치를 통해 경각심 고취시켜야 한다.

다섯째, 수탁사를 관리·감독하기 위한 일원화된 조직 구성이 필요하다. 기업에서는 개인정보 처리 업무를 위해 수십 개의 수탁사가 존재할 수 있다. 하지만, 각각의 수탁사의 계약 및 관리부서가 분리되어 있다면 개인정보보호를 위한 효과적인 관리·감독이 어려울 것이다. 따라서, 위탁업무의 계약서 관리, 제공되는 개인정보 항목, 개인정보 암호화, 재위탁 금지, 개인정보 이용 실태, 고객 민원 및 사고 발생 시 신속한 처리, 수탁사 개인정보보호 실태조사 및 제재 등 개인정보의 수집, 보관, 이용 및 제공 파기의 전 단계를 체계적으로 관리·감독하기 위해서는 이를 통합적으로 관리할 수 있는 일원화된 조직의 구성이 필요하다. 따라서, 기업은 개인정보보호 또는 정보보호 조직에 수탁사 관리·감독을 전담시키거나 별도의 관리 조직을 구성해야 한다.

4.2 개인정보보호 수탁사 관리체계를 위한 법률 강화

2.3.1에서는 언급했듯이 정보통신망법과 개인정보보호법에서는 위탁사는 수탁사가 개인정보를 안전하게 처리하는지에 대하여 감독하도록 명시하고 있다. 좀 더 자세히 살펴보면, 개인정보보호법 제26조 1항 및 시행령 제28조에서는 개인정보 처리업무 위탁 시에는 “위탁업무 수행 목적 외 개인정보의 처리 금지”, “개인정보의 기술적·관리적 보호조치”, “위탁업무의 목적 및 범위”, “재위탁 제한”, “안전성 확보 조치”, “개인정보의 관리 현황 점검 등 감독”, “손해배상 등 책임”에 대한 사항이 포함된 문서에 의하여야 하며, 동법 제28조 4항에서는 수탁자가 개인정보를 안전하게 처리하는지를 감독해야 한다고 명시하고 있다. 정보통신망법 제25조에서는 단순히 수탁사를 관리·감독해야 한다고만 명시하고 있다. 이와 같이 개인정보보호법에

〔표 26〕 법률 이슈 및 개선 방향

구분	정보통신망법	개인정보보호법
현행법	○제25조(개인정보의 취급위탁)	○제26조(업무위탁에 따른 개인정보의 처리 제한)
이슈	○수탁사 관리·감독에 대한 점검항목, 점검횟수 등에 대한 구제적인 방법이 명시되어 있지 않음	○시행령(제28조)에 점검사항에 대하여 명시하고 있으나 기술적·관리적 보호조치에 국한되어 있음
법 개선방향	○개인정보 라이프싸이클 전반에 걸친 수탁사 점검 항목 신규 추가 ○점검 횟수/년 신규 추가 ○수탁사 점검에 대한 구체적인 방법 추가	○개인정보 라이프싸이클 전반에 걸친 수탁사 점검 항목 신규 추가 ○점검 횟수/년 신규 추가

서는 위탁사가 수탁사의 개인정보처리에 대한 안전성을 감독하기 위한 사항을 법과 시행령에 명시하고 있으나, 그 기준이 기술적·관리적 보호조치에 국한되어 있어 개인정보 수집·저장·이용·파기의 라이프싸이클 전반의 보안수준을 파악하기 힘들다. 또한, 단순히 관리·감독 의무만 명시하고 있을 뿐 방법 등에 대해서는 구체적으로 명시하고 있지 않아 위탁사가 자의적으로 해석할 소지가 있다. 정보통신망법에서는 단순히 관리·감독 의무만 명시하고 있을 뿐 그 구체적인 방법, 점검항목 등의 기준이 없어 수탁사 관리·감독에 혼란을 발생 시킬 가능성이 있다. 이와 같은 법률 이슈에 따른 문제점은 3장의 수탁사 보안수준 점검결과(대부분의 수탁사 개인정보보호 수준이 낮은 것으로 확인됨)에서도 확인할 수 있다.

따라서, 법의 실효성을 높이고 개인정보보호 수탁사 관리체계를 강화하기 위해 개인정보보호법과 정보통신망법에 개인정보 수집·저장·이용·파기의 라이프싸이클 전반에 대한 점검항목과 년1회 이상 정기적인 점검 의무화를 추가시킬 필요성이 있다.

V. 수탁사 개인정보보호 관리체계 검증

본 논문에서 제안한 수탁사 개인정보보호 관리체계에 대한 그 실효성 검증방법은 수탁사를 위한 내부관리계획 표준양식 배포 및 표준 계약서, 수탁사의 체계적인 관리를 위한 조직구성, 수탁사의 개인정보 취급자 대상 집체교육, 수탁사 개인정보보호 실태점검 프로세스, 수탁사 점검 결과를 통한 벌점 부과 및 제재의 필요성 및 수탁사 점검항목에 대한 적합성 여부를 판단하고자 실제 1년 이상 수탁사 관리 및 보안 업무를 담당하는 인력 40명을 대상으로 E-mail 또는 직접 설문 방법을 사용하였으며, 1차 점검에 참여했던 4개 위탁사와 65개 수탁사를 대상으로 사례 검증을 실시하였다.

5.1 수탁사 개인정보보호 관리체계 검증 결과

설문 검증 결과는 〔표 27〕, 〔표 28〕과 같이 도출되었다. 수탁사 개인정보보호 관리체계에 대한 필요성 설문 검증은 답변항목에 대하여 "필요", "불필요"로 정리하였다. 〔표 27〕과 같이 수탁사를 위한 내부관리계획 표준양식 배포 및 표준 계약서의 필요성(97.5%), 체계적인 관리를 위한 조직구성의 필요성(92.5%), 수탁사의 개인정보 취급자 대상 집체교육의 필요성(90.0%), 수탁사 개인정보보호 실태점검 프로세스의 필요성(95.0%), 점검 결과를 통한 벌점 부과 및 제재의 필요성(92.5%)에 대하여 90%이상이 필요하다는 결과가 도출되었다. 수탁사의 개인정보취급자에 대해서 위탁사가 정보보호 집체 교육을 진행해 줄 필요는 없다는 응답도 있었으나 기본적으로 수탁사 개인정보

〔표 27〕 수탁사 개인정보보호 관리체계의 필요성 설문 검증 결과

제안 항목	의견	정보보호 담당자	구매팀 담당자	개인정보 관리 책임자	소계
수탁사를 위한 내부관리계획 표준양식 배포 및 표준 계약서	필요	25	9	5	39 (97.5%)
	불필요	0	1	0	1 (2.5%)
체계적인 관리를 위한 조직구성	필요	24	8	5	37 (92.5%)
	불필요	1	2	0	3 (7.5%)
수탁사의 개인정보 취급자 대상 집체교육	필요	23	8	5	36 (90.0%)
	불필요	2	2	0	4 (10.0%)
수탁사 개인정보보호 실태점검 프로세스	필요	25	8	5	38 (95.0%)
	불필요	0	2	0	2 (5.0%)
점검 결과를 통한 벌점 부과 및 제재	필요	23	9	5	37 (92.5%)
	불필요	2	1	0	3 (7.5%)

보호 관리체계의 중요성에 대해서는 “동감한다“는 의견이었다.

점검항목 설문 검증은 답변항목에 대하여 “매우필요”, “필요”, “보통”, “필요없음”, “전혀필요없음”의 5개 항목으로 “매우필요”, “필요”는 〈적합〉, “보통”은 〈보통〉, “필요없음”, “전혀필요없음” 은 〈부적합〉으로 정리하였다. 〔표 28〕과 같이 개인정보보호 내부관리계획 및 개인정보(100.0%), 개인정보취급자 관리(92.5%), 개인정보 저장 및 관리(87.5%), 개인정보 처리(83.8%), 개인정보 제공(100.0%), 개인정보 파기(90.0%), 시스템 보호(86.3%), 열람/정정/삭제 대응(87.5%)의 8개 도메인에 대하여 적합하다는 결과가 도출되었다. 대부분의 항목이 90%이상 적합하다는 결과가 도출되었지만, 개인정보 처리, 시스템 보호의 필요성에 대해서는 부적합 의견이 다소 존재하는데 이는 법률에서 요구하는 안정성 확보조치에 대한 이해가 부족하기 때문인 것으로 파악된다.

〔표 28〕 점검항목 설문 검증 결과

도메인	점검항목	점검항목 타당성 검증			소개
		적합	보통	부적합	
개인정보 보호 내부관리 계획 및 개인정보	개인정보관리책임자 지정 및 위탁사 통보 여부	40			40
	개인정보보호 내부관리계획 수립 여부	40			
	개인정보취급방침 보유 여부	40			
	점검항목 응답률	100.0%			100.0%
개인정보 취급자 관리	개인정보취급자 현황관리	37	3		40
	개인정보취급자에대한교육여부 (년2회)	36	3	1	
	개인정보취급자 채용 시 보안서약서 작성 여부	38	2		
	점검항목 응답률	92.5%	6.7%	0.8%	100.0%
개인정보 저장 및 관리	개인정보의 저장 및 전송 시 암호화 여부	37	3		40
	개인정보가 포함된 문서를 보안장치가 설치된 장소에 보관하고 있으며, 문서이관 시 보안절차 시행 여부	33	5	2	
	점검항목 응답률	87.5%	10.0%	2.5%	100.0%
개인정보 처리	개인정보처리시스템 접근내역 저장 유무	35	3	2	40
	개인정보의 출력/복사시 출입/복사관리대장기록 및 개인정보관리책임자의 승인 유무	32	5	3	
	점검항목 응답률	83.8%	10.0%	6.3%	100.0%
개인정보 제공	위탁사로부터 제공받은 개인정보의 재위탁 또는 제3자 제공 여부	40			40
	점검항목 응답률	100.0%			100.0%
개인정보 파기	개인정보(문서,데이터파일형태)의 이용목적 달성 후 개인정보 파기규정에 따른 지체없이 파기와 결과에 대한 위탁사 통보 여부	37	3		40
	개인정보파일 삭제 시 파일완전삭제 프로그램의 사용 여부 및 장치 폐기 시 물리적 완전파괴 방법 사용 여부	35	3	2	
	점검항목 응답률	90.0%	7.5%	2.5%	100.0%
시스템 보호	개인정보취급자의 접속기록 위/변조 방지를 위한 정기적인 백업수행 여부	35	3	2	40
	개인정보처리시스템 계정 또는 업무용PC사용자 이력관리 여부	35	5		
	개인정보취급자의 인사이동 및 퇴직 시 접근권한 변경 및 말소 처리 여부	38	2		
	개인정보처리시스템 및 업무용PC에 대한 접근통제장치 설치 여부	30	6	4	
	점검항목 응답률	86.3%	10.0%	3.8%	100.0%
열람/정정/삭제 대응	정보주체가 자신의 개인정보에 대한 열람/정정/삭제 등의 요구 시 조치절차 수립 여부	35	4	1	40
	정보주체가 자신의 개인정보의 이용 및 처리정지 요구 시 이에 대한 조치절차 수립 여부	35	4	1	
	점검항목 응답률	87.5%	10.0%	2.5%	100.0%

5.2 수탁사 개인정보보호 관리체계 사례 검증 결과

수탁사 개인정보보호 관리체계 프로세스의 실제 적용 결과를 확인하기 위해 1차 점검에 참여했던 4개 위탁사와 65개 수탁사를 대상으로 사례 검증을 실시하였다. 사례 검증 방법은 〔표 29〕와 같다.

그 결과 〔표 30〕과 같이 평균 보안수준은 87.0%로 최초 실태조사 때의 45.5%보다 약 42% 상승되었음

〔표 29〕 사례 검증 방법

구분	상세 내용	비고
대상	○위탁사 : 4개 ○수탁사 : 65개	1차 점검 대상
조직구성	○위탁사 별 수탁사 관리감독 조직구성(정보보호팀)	
1차 점검 결과 통보	○1차 점검 결과 수탁사에 통보	
표준양식 제공	○개인정보보호 내부관리계획서 표준 양식 제공 ○표준 위탁 계약서를 통한 재계약	
집체 교육	○수탁사의 개인정보취급자를 대상으로 집체교육 진행	
재점검 및 결과 통보	○재점검 실시 및 보안수준 분석 ○수탁사에 결과 통보 및 이행계획서 요청	보안수준분석 방법 : 〔표 5,6,7,8〕
이행 결과 확인	○재점검 결과에 대한 이행 유무 확인	
제재 기준 적용	○및 이행 결과를 종합 평가하여 제재 기준 적용	

〔표 30〕 도메인별 보안수준 재점검 결과

점검 도메인	1차점검	재점검
개인정보보호 내부관리계획 및 개인정보취급방침 수립	48.2%	91.3%
개인정보 취급자 관리	46.5%	84.0%
개인정보 수집	N/A	N/A
개인정보 저장 및 관리	49.2%	85.2%
개인정보 처리	46.6%	80.9%
개인정보 제공	90.0%	100.0%
개인정보 파기	32.9%	83.4%
개인정보처리시스템의 보호조치	44.2%	87.1%
개인정보 열람/정정/삭제 요구 대응	33.1%	89.2%
평균	45.5%	87.0%

을 확인 할 수 있었다. 특히, 개인정보보호 내부관리계획 및 개인정보취급방침 수립, 개인정보취급자 관리, 개인정보 열람/정정/삭제 요구 대응 부분의 보안수준이 크게 증가하였는데, 이는 위탁사에서 제공한 표준 개인정보보호 내부관리계획이 반영되고 수탁사 개인정보 취급자에 대한 집체교육이 진행되었기 때문인 것으로 분석될 수 있다. 도메인별 보안수준 재점검 결과는 〔표 31〕과 같다.

세부결과를 살펴보면 개인정보보호 내부관리계획 및 개인정보취급방침 수립, 개인정보취급자 관리, 개인정보 처리, 개인정보 제공, 개인정보 열람/정정/삭제 요구 대응 부분은 이행완료 비율이 높은 편이나 개인정보 파기, 개인정보처리시스템의 보호조치 부분과 같이 시스템적으로 보안을 적용해야하는 부분은 현실적으로 즉시 이행이 불가능한 부분이 다수 존재하여 이행계획서제출 비율이 높은 것으로 확인되었다. 따라서, 반드시 위탁사는 수탁사가 이행계획서의 내용에 따라 보안적용을 완료 했는지 확인할 필요가 있다.

〔표 31〕 보안수준 재점검 세부결과

도메인	점검항목	이행 완료	이행계획 제출	미이행
개인정보 보호 내부관리 계획 및 개인정보 취급방침 수립	개인정보관리책임자 지정 및 위탁사 통보 여부	60 (92.3%)	0 (0%)	5 (7.7%)
	개인정보보호 내부관리계획 수립 여부	59 (90.8%)	0 (0%)	6 (9.2%)
	개인정보취급방침 보유 여부	59 (90.8%)	0 (0%)	6 (9.2%)
개인정보 취급자 관리	개인정보취급자 현황관리	50 (76.9%)	2 (3.1%)	13 (20.0%)
	개인정보취급자에 대한 교육 여부(년2회)	56 (86.2%)	0 (0%)	9 (13.8%)
	개인정보취급자 채용 시 보안서약서 작성 여부	56 (86.2%)	5 (7.7%)	4 (6.2%)
개인정보 수집	개인정보 수집항목	N/A	N/A	N/A
개인정보 저장 및 관리	개인정보의 저장 및 전송 시 암호화 여부	54 (83.1%)	0 (0%)	10 (15.4%)
	개인정보가 포함된 문서를 보안장치가 설치된 장소에 보관하고 있으며, 문서 이관 시에 보안절차 시행 여부	55 (84.6%)	0 (0%)	9 (13.8%)
개인정보 처리	개인정보처리시스템 접근내역 저장 유무	57 (87.7%)	0 (0%)	8 (12.3%)
	개인정보의 출력/복사 시에 출입/복사 관리 대장 기록 및 개인정보관리책임자의 승인 유무	57 (87.7%)	0 (0%)	8 (12.3%)
개인정보 제공	위탁사로 부터 제공받은 개인정보의 재위탁 또는 제3자 제공 여부	65 (100%)	0 (0%)	0 (0%)
개인정보 파기	개인정보(문서, 데이터 파일 형태)의 이용목적 달성 후 개인정보파기 규정에 따른 지체 없이 파기와 파기결과에 대한 위탁사 통보 여부	55 (84.6%)	0 (0%)	10 (15.4%)
	개인정보파일 삭제 시 파일완전삭제 프로그램의 사용 여부 및 장치폐기 시 물리적 완전파괴 방법 사용 여부	53 (81.5%)	0 (0%)	12 (18.5%)
개인정보 처리 시스템의 보호조치	개인정보취급자의 접속기록 위/변조 방지를 위한 정기적인 백업 수행 여부	60 (92.3%)	2 (3.1%)	3 (4.6%)
	개인정보처리시스템 계정 또는 업무용PC사용자 이력 관리 여부	48 (73.8%)	1 (1.5%)	16 (24.6%)
	개인정보취급자의 인사이동 및 퇴직 시 접근권한 변경 및 말소처리 여부	58 (89.2%)	4 (6.2%)	3 (4.6%)
	개인정보처리시스템 및 업무용PC에 대한 접근통제 장치 설치 여부	56 (86.2%)	0 (0%)	9 (13.8%)
개인정보 열람/정정 /삭제 요구 대응	정보주체가 자신의 개인정보에 대한 열람/정정/삭제 등의 요구 시 조치절차 수립 여부	58 (89.2%)	0 (0%)	7 (10.8%)
	정보주체가 자신의 개인정보의 이용 및 처리정지 요구 시 이에 대한 조치절차 수립 여부	58 (89.2%)	0 (0%)	7 (10.8%)

재점검 결과, 이행결과, 이행계획서를 통해 수탁사의 보안수준을 종합적으로 분석한 결과 〔표 32〕와 같다. 벌점 적용은 미이행 1점, 이행계획서제출 0.5점을 부과하였으며, 총 벌점이 0점인 수탁사는 17개, 1~4점인 수탁사는 40개, 5~8점인 수탁사는 3개, 9점 이

〔표 32〕 총 벌점 및 제재기준 적용 결과

총 벌점	결과	비고	
0점	26.2%(17개)	-	계약 유지
1~4점	61.5%(40개)	주의	
5~8점	4.6%(3개)	경고	
9점 이상	7.7%(5개)	계약해지	

상인 수탁사는 5개로 확인되었다. 이에 따라, 총 벌점이 9점 이상인 5개의 수탁사에 대해서는 계약을 해지하였으며 해당 서비스에 대해서는 새로운 수탁사를 선정하였다.

VI. 결 론

개인정보 생명주기 단계에서 기업 스스로가 직접적으로 개인정보를 보호할 수 있는 단계는 수집(수집 위탁 제외), 저장, 이용, 파기단계이다. 하지만, 제공단계(개인정보 처리 위탁)는 기업이 정보주체로부터 수집한 개인정보를 타인 즉, 제3자에게 제공하므로 제3자를 통제하지 못하면 개인정보가 유출될 가능성이 존재 할 수 있다. 또한, 기업의 서비스 특성상 개인정보 처리 업무 위탁을 위한 수탁사가 증가할수록 개인정보 유출가능성은 높아진다고 할 수 있다.

본 연구에서는 그동안 개인정보 처리 위탁 부분에서 전혀 제기되고 있지 않았던 개인정보보호에 관한 법률적 검토와 수탁사들에 대한 개인정보보호 실태를 분석하고 문제점을 도출하였다. 이러한 분석을 토대로 기업이 개인정보보호를 위해 수탁사들을 보다 효율적으로 관리·감독할 수 있는 위한 방안으로 수탁사 내부관리계획 수립을 위한 표준양식 마련, 수탁사 개인정보 취급자를 대상으로 주기적인 개인정보보호 및 정보보호 교육, 수탁사에 대한 개인정보보호 실태점검 프로세스 수립, 수탁사 관리·감독 및 통제를 위한 기준 마련, 조직의 일원화라는 개선 방안과 법률 개선방안을 제시하였다. 또한, 개인정보보호를 위한 수탁사 관리체계에 대한 사례 검증 결과, 1차 점검 시 45.5%였던 보안수준이 87.0%로 약 42% 상승되었음을 확인하였다. 따라서 위탁사의 관리·감독이 강화 될수록 수탁사의 개인정보보호 수준이 증가되고 그 결과 개인정보 유출 가능성도 낮아짐을 확인하였다.

기업은 본 연구에서 제시한 개인정보보호를 위한 수탁사 관리체계 강화 방안을 통해 법적 준거성을 만족시키고 개인정보 처리업무 위탁 시 발생할 수 있는 개인정보 유출사고를 미연에 방지할 수 있을 것이다.

참고문헌

〔1〕 한국인터넷진흥원, "2013 국가정보보호백서", pp. 125, 2013년 4월.
〔2〕 한국인터넷진흥원, "2012년 12월 인터넷 침해사고 대응통계 월보", 2013년 1월.
〔3〕 법제처, "서울중앙지방법원 2011.1.17., 선고, 2010노 2850, 판결", 2011년 1월.
〔4〕 법제처, "수원지법 2005.7.29., 선고, 2005고합 160, 판결:확정", 2005년 7월.
〔5〕 행정안전부, "표준 개인정보보호 지침", pp. 7, 2011년 9월.
〔6〕 행정안전부, "개인정보 보호법령 및 지침고시 해설", pp. 94, 2011년 12월.
〔7〕 개인정보분쟁조정위원회, "2004년 개인정보 분쟁조정 사례집", pp. 223, 2004년 12월.
〔8〕 한국인터넷진흥원, "2012년 정보보호 실태조사(기업편)", pp. 104, 2013년.

〈저자소개〉

강 태 훈 (Tae-hun Kang) 정회원
2008년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호정책, 개인정보보호, 디지털포렌식, 암호 이론 등

임 종 인 (Jong-in Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
現 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수
現 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등