Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.383

개인정보보호 강화를 위한 위탁 업무 보안관리 프레임웍 제안

고 영 대,[1,2†] 이 상 진[1‡]
[1]고려대학교, [2]법무법인 율촌

A Proposal of Enhanced Personal Information Security management Framework of Consigning of Personal Information

Youngdai-dai Ko,[1,2†] Sang-jin Lee[1‡]
[1]Korea University, [2]Attorneys at Law Yulchon

요 약

최근 개인정보를 취급하는 개인정보처리자의 비용절감, 전문성을 통한 업무효율성의 증대 및 서비스 품질 개선 등의 다양한 목적에 따라 개인정보의 처리 업무를 제3자에게 위탁하는 경우가 늘어나고 있다. 이렇듯, 정보주체의 개인정보가 개인정보처리자가 아닌 제3자에 의하여 이루어지는 위탁업무가 증가함에 따라 개인정보를 위탁받아 처리하는 수탁사에 대한 개인정보보호에 대한 관심과 노력 또한 당연히 증대되어야 할 것이다. 이에, 본 논문에서는 이러한 취지에 기반하여 개인정보 위수탁 업무 진행 시 수탁사를 위한 효율적인 관리방안 뿐만 아니라, 위탁사가 위수탁 업무 전반에 걸쳐 개인정보보호 프레임웍을 정립하고 이를 토대로 수탁 업체 선정 및 계약 단계에서부터 위수탁 업무 운영 및 관리, 위수탁 업무 계약 해지 및 종료에 이르는 각 단계에서 고려해야할 개인정보보호 요건들을 제안하고자 한다.

ABSTRACT

Recently, the number of companies consigning their personal information management work has been increasing; they consign the work for various reasons and purposes, for example, in order to reduce costs related to personal information managers, improve efficiency through professional performance and to improve service quality. As such, since the cases where an consigning agency - not the personal information manager - handles personal information are increasing due to the increase of consigning of the personal information management work, we need to concerned with and pay attention to how much such agency makes efforts for personal information protection. In this regard, this study suggests a plan for efficient management of the agency during the course of consigning work as well as a list of requirements for personal information protection to be considered in each phase of the following; establishment of personal information protection framework for all consigning work processes, selection of consigning agency, execution of consigning contract, operation and management of consigning work, and termination of contract.

Keywords: Personal Information Security, Consigning of Personal Information, Consigning agency

접수일(2015년 1월 13일),수정일(1차: 2015년 2월 3일), 게재확정일(2015년 2월 17일)

† 주저자, ydko@korea.ac.kr, ydko@yulchon.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

I. 서 론

개인정보의 위수탁 업무 유형은 기업의 개인정보 취급 목적 및 비즈니스 업태에 따라 다소 차이가 있을 수 있으나 일반적으로는 콜센터를 통한 상담 업무 대행, DM 업체를 통한 고지서 등의 배송, 전산시스템의 개발 및 유지보수 등의 다양한 형태로 나타나고 있다.

이처럼 기업의 입장에서는 고객 및 임직원 등의 개인정보를 취급함에 있어, 비용의 절감과 해당 위탁 업무에 대한 전문성 등을 고려하여 개인정보처리자의 개인정보 취급 업무 목적에 따라 다양한 유형으로 개인정보를 위탁하고 있는 실정이다.

현행 개인정보보호 관련 주요 법령인 개인정보보호법[4]과 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법")[5]에서는 이러한 개인정보의 위수탁 과정에서 발생할 수 있는 보안위협을 최소화하고 위수탁 과정의 이해당사자인 위탁사 및 수탁사가 반드시 준수해야 할 법령 의무조항들을 명시하고 있다. 특히, 방송통신위원회에서는 지난 '15년 1월 13일, 개인정보를 처리하는 사업자의 내부관리계획에 위탁사의 명확한 관리책임을 위하여 "개인정보 처리업무를 위탁하는 경우 수탁사에 대한 관리 및 감독에 관한 사항"을 추가하여 수탁사 관리·감독을 소홀히 한 경우에 대한 과징금 부과 근거를 신설하는 형태로 정보통신망법 하위 기준 고시인 개인정보의 기술적·관리적 보호조치 기준 일부 개정안을 입안예고 한 바 있다.[12] 이 밖에도 개인의 재산 및 신용과 직결되는 개인정보를 처리하고 있는 금융회사의 경우, 전자금융거래법[6] 및 신용정보의 이용 및 보호에 관한 법률(이하 "신용정보법")[7] 등에서 보다 강화된 법률 규정을 통해 개인정보의 위수탁 업무 관련하여 통제하고 있다.

이러한 개인정보 위수탁 과정에서 당연히 고려해야 할 사항 중의 하나가 개인정보를 위탁받아, 위탁사의 개인정보처리를 대행하고 있는 수탁사에 대한 개인정보보호 관리 현황인 것으로 보인다. 이에, 지금까지의 개인정보 위수탁과 관련한 연구 성과는 수탁사가 준수해야할 개인정보보호 관점의 진단항목 개발 및 수탁사의 보안관리를 위한 방향에 집중하고 있다.[1,2]

그러나, 수탁사 또한 개인정보를 위탁받아 개인정보를 처리하는 개인정보처리자의 위치에 놓여있기 때문에, 수탁사가 위에서 언급한 개인정보관련 법령을 준수하고 이에 대한 관리 방향성을 수립하여 이를 준수해야하는 것은 자못 당연한 일인 것으로 보인다. 수탁사의 개인정보 관리수준에 대한 점검 및 개선은 개인정보 처리 위탁업무 관점에서 고려해야 할 보안 요건 중 상당히 큰 비중을 차지하는 것은 당연한 이치이지만, 이 부분이 개인정보 처리 위탁업무에 대한 개인정보보호 강화를 위한 필수 보안 요건 중의 전체가 아닌 일부 필수 항목 중의 하나로 정의되고 관리될 필요가 있다. 이는 개인정보의 위수탁이라는 업무 자체가 수탁사의 개인정보보호 수준 뿐만아니라, 위탁사가 행하고 있는 위탁사 전체의 개인정보보호 활동과 연계되어야 함은 물론이거니와, 위수탁 과정에서 반드시 일어나는 수탁사 선정 및 계약, 위수탁 업무의 이행, 계약 해지 및 위수탁 업무의 종료 등 위수탁 업무 전반적인 관점에서 살펴볼 필요가 있기 때문이다.

본 논문에서는 이러한 취지에 기반하여 개인정보 위수탁 업무 진행 시 기존 연구 성과물들에서 주로 살펴본 수탁사를 위한 진단항목 및 관리기준 뿐만 아니라, 위탁사가 위수탁 업무 전반에 걸쳐 반드시 고려해야 할 개인정보보호 프레임웍을 정립하여 이를 토대로 수탁 업체 선정 및 계약 단계에서의 개인정보보호 조치와 위수탁 업무 운영 및 관리 단계에서의 개인정보보호 조치, 위수탁 업무 계약 해지 및 종료 단계에서의 개인정보보호 조치를 마련하기 위한 방안을 제시하고자 한다.

II. 선행 연구

2.1 연구 사례

지금까지의 개인정보의 처리 업무를 위탁받아 정보주체의 개인정보 취급업무를 대행하고 있는 수탁사의 개인정보보호 관리체계 강화를 위한 연구[1, 2]는 주로 수탁사를 위한 진단 및 감사 방향에 초점을 맞추어 진행되었다. 수탁사를 개인정보 수탁 업무 유형에 따라 분류하고 수탁사가 개인정보보호 관련 법령에 따라 준수해야할 의무조항을 도출하였다. 또한 개인정보보호 관련 인증제도인 ISMS, PIMS 등에서 법령 상 의무 조항은 아니더라도 개인정보보호 향상을 위하여 필요한 요건들을 도출하여 수탁사 진단항목을 개발하고 이를 토대로 수탁사를 진단하고 해당 진단 결과를 분석하여 이러한 의무조항의 타당성을 이끌어내는 방식을 적용하였다.

▪ 개인정보보호 수탁사 관리체계 강화 방안 연구[1]

[1]에서는 개인정보 처리업무의 위탁과 제3자 제공

의 구분을 위해 다양한 유형의 개인정보 위수탁 업무에 대한 서비스를 분류하고, 개인정보 위수탁 시 고려해야 할 법률 요건들에 대하여 정의하였다. 이를 토대로 수탁사의 개인정보보호 실태분석을 위한 수준분석 방법을 제시하였고, 〔표1〕[1]과 같이 65개사에 달하는 수탁사의 개인정보보호 수준분석을 통해 세부 진단 결과에 대한 분석 및 향후 수탁사의 개인정보보호를 위한 관리체계 수립을 위한 방안을 제시한 바 있다.

〔1〕은 수탁사가 취해야할 개인정보보호 요건을 도출하고 이러한 요건에 따라 실제 각 수탁사별 개인정보보호 실태조사 및 결과 분석이라는 점에서 시사하는 바가 크다고 할 수 있다.

Table 1. Security Level by Inspection Domain

Inspection Domain	Security Level
Internal Management Plan of Personal Information Protection and Establishment of Policy on Handling of Personal Information	48.2%
Management of Personal Information Handler	46.5%
Collection of Personal Information	NA
Storing and Management of Personal Information	49.2%
Handling of Personal Information	46.6%
Provision of Personal Information	90.0%
Disposal of Personal Information	32.9%
Protection Measures of Personal Information Handling System	44.2%
Responding to Reference/ Correction/ Deletion Request of Personal Information	33.1%
Average	45.5%

▪ 금융회사 개인신용정보 수탁사에 대한 관리 감독 현황 및 개선 방향에 관한 연구〔2〕

〔1〕에서 언급한 '개인정보보호 수탁사 관리체계 강화 방안 연구'가 일반적인 개인정보처리자 관점에서 개인정보 위수탁 업무 과정에서 필요한 바를 서술하였다면, 〔2〕에서는 금융회사의 개인(신용)정보 관점에서의 개인정보 위수탁 과정에서 고려해야 할 바를 중점적으로 언급하고 있다.

특히, 금융회사에 위수탁 업무 중 DM 및 CD/ATM VAN 업무를 위탁받아 처리하고 있는 수탁사를 위한 진단항목을 도출하고 이러한 진단항목에 따라 수탁사로써 개인정보보호 활동을 이행하고 있는지에 대하여 조사하고 이를 통한 수탁사 개인정보보호 현황을 분석하는 등 금융회사 업종을 고려한 수탁사 진단항목을 도출하는 성과였다.

뿐만 아니라, 〔2〕에서는 국외 업무위탁 정보보호 관리·감독 사례를 분석하여 소개하고 있으며, 이를 인용하자면, 미국 금융회사의 경우 업무위탁에 대한 금융회사의 자체 보안프로그램(Self-Assessment program)을 통해 보안수준에 대한 적정성을 평가하고 있고〔9〕, 미국의 BITS(Banking Industry Technology Secretariat)에서는 아웃소싱업체에 대한 관리 및 보안평가를 위해 아웃소싱 업체를 회원으로 가입하도록 하여 자체평가 프로그램(Shared - Assessment Program)을 전문평가업체인 Deloitte, EY, KPMG, PWC 등의 전문기관 평가를 통해 보안수준을 관리 하도록 하고 있으며〔10〕 또한, 유럽의 경우, 2012년 EU 개인정보보호지침을 EC Directive에서 구속력이 존재하는 Regulation 형태로 제재 수위를 강화하려 하고 있으며 개인정보에 대한 해외 이전 등과 같은 정보의 이동 등에 대해 국가의 개인정보보호 수준(Adequate level of protection)을 평가하여 허가하는 등의 개인정보에 대한 외부 제공에 대한 사항을 강도 높게 제한하고 있다[2]〔11〕고 언급하고 있다.

2.2 주요 시사점 및 연구 방향

앞서 언급한 주요 논문의 경우 각각 개별적으로 개인정보 위수탁 시 고려해야 할 기준 및 세부 사항 등에 대해 언급하고 있으며, 특히 위탁사 입장에서 수탁사의 개인정보보호 수준을 진단하고 위탁사가 개인정보를 위탁함에 있어서 수탁사로써, 이러한 개인정보를 관련 법령에 근거하여 안전하게 처리 및 관리하고 있는지에 대해 점검할 수 있는 합리적인 기준 요건들을 제시하였다는 점에서는 의미가 크다고 할 수 있다.

그러나, 수탁사의 경우, 개인정보 처리 위탁이라는 업무적 특수성을 감안하여 개인정보 처리범위가 위탁사의 개인정보 취급업무의 일부분에 해당할 수는 있으나, 수탁사 또한 개인정보 처리자로서 준수해야 할 사

1) 강태훈, 개인정보보호 수탁사 관리체계 강화 방안 연구, 786페이지

2) 이용진, 금융회사 개인신용정보 수탁사에 대한 관리 감독 현황 및 개선 방향에 관한 연구, 235페이지

항은 위탁사가 개인정보보호 관련 법령에서 규율하는 내용과 크게 다르지 않고 개인정보 처리 위탁 업무범위에 따라 오히려 제한적일 수 있다.

즉, 개인정보 처리 위탁업무와 관련한 개인정보보호 강화라는 관점에서 살펴본다면, 수탁사의 개인정보보호 관리 수준에 대한 진단 및 개선은 위탁사가 반드시 고려해야할 항목이긴 하나, 개인정보 위수탁 업무 과정에서 필요한 필요 요건의 성격이지, 충분조건은 아니라는 점을 이해할 수 있다. 개인정보 위수탁 업무란 개인정보를 위탁할 업체의 합리적인 선정 기준을 통해 해당 수탁사를 선정하고, 이러한 기준 하에 선정된 수탁사와 개인정보보호를 위한 계약의 체결을 통해, 본격적인 위수탁 업무가 진행되고, 업무 목적이 다한 경우 해당 위수탁 업무에 대한 계약 해지 및 위수탁 업무가 종결되는 일련의 Life-Cycle을 갖는데, 현재까지의 주요 관심사항은 위수탁 업무가 진행되는 과정에서 수탁사의 실태점검을 위한 부분에 중점되었기 때문이다.

이에 본 논문에서는 개인정보 위수탁이 이루어지는 전체 과정을 하나의 비즈니스 업무 프로세스로 분석하여 위수탁 업체의 선정 및 계약 단계에서부터, 위수탁 업무에 대한 이행 및 계약 해지 및 종료에 이르는 전반적인 과정에서 필요한 사항들을 정립하여, 개인정보를 처리하는 위탁사 및 수탁사들이 준수해야할 보안 요건들에 대한 방향성을 수립하고자 하였다.

III. 개인정보 위수탁 보안관리 프레임웍

3.1 개요

본 논문에서 제안하고자 하는 개인정보 위수탁 보안관리 프레임웍은 [그림 1]과 같은 형태로 구성하였다.

첫 번째 단계에서는, 개인정보 위수탁 업무에 따라 고려해야할 개인정보보호 관련 법적 또는 제도적 기본 요건들을 도출하고자 하였다. 이러한 기본 요건

들에 기반하여 두 번째 단계에서는, 위수탁 업체 선정 및 계약에서부터, 위수탁 업무 이행 및 위수탁 업무의 계약 해지 및 종료에 이르는 위수탁 업무 전반적인 과정에서 개인정보보호 관련 이슈사항을 식별하고 점검 및 개선하고자 하였다.

또한, 이러한 위수탁 업무에 따른 개인정보보호 활동이 조직 전체의 개인정보보호 변화관리 활동과 연계될 수 있도록 마지막 단계로, 전사적 개인정보보호 관리체계와의 연계 방향을 마련하는 형태로 개인정보 위

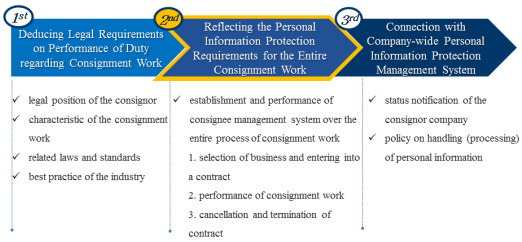

Fig. 1. Composition Direction of Personal Information Security Management Framework for Consignment Work

수탁에 따른 보안관리 프레임웍을 구성하였다.

3.1.1 위수탁 업무에 따른 개인정보보호 요건 도출

개인정보 위수탁 업무 관련 Compliance 충족을 위하여 필요한 법률 요구사항 분석은 개인정보보호 요건 정의를 위한 필수 불가견의 항목이라 할 수 있다. 선행 연구 사례에서 살펴본 연구[1,2]에서도 이러한 관련 법령에 근거한 수탁사별 개인정보보호를 위한 법령 분석 및 이를 토대로 진단항목을 도출한 바 있다. 일반적인 개인정보처리자로서의 의무 이행 법률 조항을 제외한 개인정보의 위수탁 업무 이행과정에 부합하는 주요 관련 법령 및 조항들은 [표 2]와 같다.

개인정보 위수탁 관련 법률 규정 이외에 개인정보처리자로서 당연히 준수해야 할 개인정보보호 관련 법규 항목들에 대해서는 본 논문에서 제시하고자 하는 위수탁 업무에 대한 개인정보보호 강화라는 취지와 다소 차이가 있어 구체적인 언급은 생략하였으나, 이러한 항목들 또한 개인정보처리자로서 위탁사 및 수탁사들 모두가 준수해야한다.

Table 2. Laws Related to Consignment Work

Major Laws	Provisions of Related Regulations
▪ Personal Information Protection Act	Article 26 (Restrictions on Management of Personal Information Following Entrustment of Affairs)
▪ Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.	Article 25 (Entrusted Handling of Personal Information)

Major Laws	Provisions of Related Regulations
▪ Use and Protection of Credit Information Act	Article 17 (Entrustment of Collection, Investigation and Processing) Article 32 (Consent to Provision and Use of Personal Credit Information)
▪ Electronic Financial Transactions Act	Article 40 (Supervision and Inspection of Financial Institutions, etc. over Affiliations or Outside Orders)
▪ Regulation on Outsourcing of Information Processing and IT Facilities of Financial Companies	Article 4 (Entrustment of Information Processing)~ Article 8 (Supervision and Inspection)

3.1.2 위수탁 업무 전반 개인정보보호 요건 반영

위수탁 업무 전반에 걸쳐 개인정보보호 요건을 반영하기 위한 〔2nd〕단계는 본 논문에서 제시하고자 하는 개인정보보호 강화를 위한 위수탁 업무의 보안관리 프레임웍에서 핵심 부분을 차지한다고 할 수 있다. 3.1절에서도 언급한 바와 같이 본 논문에서는 위수탁 업무 과정을 '위수탁 업체 선정 및 계약' 단계, '위수탁 업무 진행' 단계 및 '위수탁 업무의 계약 해지 및 종료'의 3단계로 구분하고 각 과정별로 반드시 다루어져야 할 개인정보보호 요건들을 고려하였다.

① '위수탁 업체 선정 및 계약' 단계
- ✓ 업체 선정 기준 및 계약 관계 정의
- ✓ 업무 이행 범위 정의
- ✓ 수탁사 관리감독 기준마련

② '위수탁 업무 진행(운영 및 관리감독)' 단계
- ✓ 수탁사 현황 분류 및 관리기준 수립
- ✓ 수탁사 진단 및 평가체계 운영

③ '위수탁 업무의 계약 해지 및 종료' 단계
- ✓ 위수탁 업무의 이관
- ✓ 계약 해지에 따른 보안 관리 적용

위수탁 업무 전반에 걸친 개인정보보호 요건과 관련한 상세 내용에 대해서는 이후 IV장에서 보다 자세하게 다루기로 하며, 본 절에서는 IV장에서 다루고자 하는 기본 방향성에 대해서만 언급하기로 한다.

3.1.3 개인정보보호 관리체계와의 연계

일반적으로 개인정보를 처리하는 조직의 경우, 수준의 차이는 있을지언정 나름의 개인정보보호를 위한 기본적인 관리체계를 수립하여 조직의 개인정보보호 활동을 전개하고 있다. 개인정보보호법이 발효된 지난 2011년 9월 이후부터 행정자치부 및 방송통신위와 같은 규제당국의 각종 가이드라인 제시와 지속적인 실태조사의 결과에 따른 현상이다. 이렇듯, 개인정보를 처리하는 개인정보처리자의 경우 전사적인 개인정보보호 관리체계를 운영하고 있다는 가정하에, 개인정보 위수탁에 따른 보안관리 활동 또한 조직의 개인정보보호 활동과 자연스레 연계됨이 바람직하다 할 것이다. 이를 위해 본 논문에서는 개인정보 위수탁 업무 보안관리 프레임웍의 마지막 축으로 전사 개인정보보호 체계와의 연계를 위한 변화관리 항목을 제시하고자 한다.

앞서 3.1.1절의 위수탁 업무에 따른 개인정보보호 요건에서 도출한 바와 같이 정보주체의 개인정보를 위탁하는 경우 해당 정보주체에게 관련 사실을 고지하고 이를 개인정보취급방침에 반영하는 등의 전사적인 관점에서의 개인정보보호 관리체계와 연계가 필요하다.

즉, 개인정보 위수탁 관련 법령 및 내부 정보보호 기준의 변화에 맞추어, 위수탁 관련 개인정보보호 요구사항의 기준 요건 변경, 위수탁 업체 현황 및 위수탁 업무 목적 및 범위 변경 등에 따른 정보주체의 고지 의무 이행 및 개인정보처리방침 변경 등에 필요한 제반 사항들에 대해 전사 개인정보보호 관리체계와 〔그림 2〕와 같은 유기적인 연관성을 고려하여야 할

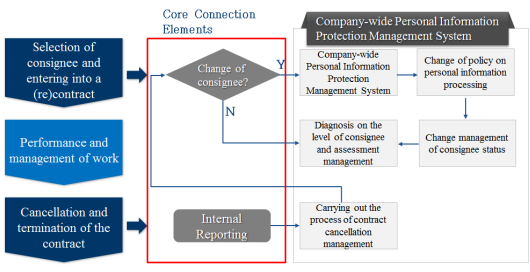

Fig. 2. Plan for Connection with Personal Information Protection Management System

것이다.

3.2 개인정보 위수탁 보안관리 프레임웍

3.1절에서 언급한 측면들을 종합하여 본 논문에서 제안하고자 하는 개인정보보호 강화를 위한 위수탁 업무 보안관리 프레임웍을 구성하고 있는 주요 모듈을 소개하면 〔그림 3〕과 같다.

첫째, 법/제도적인 관점에서 개인정보의 위수탁 업무 관련한 기본 개인정보보호 요건들을 기반 요구사항으로 도출하였고, 둘째, 이를 토대로 위수탁 업체 선정 및 계약에서부터 위탁업무 운영, 관리감독, 위수탁 업무의 계약 해지 및 종료에 이르기까지의 제반 과정에 필요한 개인정보보호 요구사항들과 마지막으로 이러한 위수탁 과정에서의 개인정보보호 이행활동들이 개인정보처리자 입장의 전사적인 개인정보보호 활동과의 전사적인 변화관리 차원에서 고려되어야할 요건들을 반영하였다. 특히, 두 번째 위수탁 업무 보안관리 프레임웍으로 제시한 위수탁 업무 이행 과정 제반 과정에 걸친 개인정보보호 요구사항에 대해서는 다음 장에서 보다 상세히 다루고자 한다.

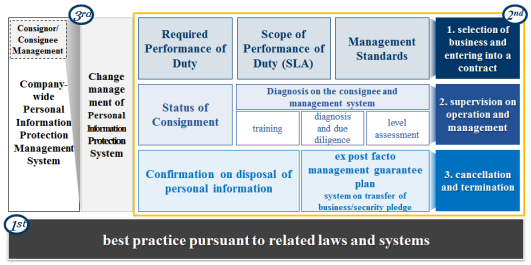

Fig. 3. Framework on Security Management of Consignment Work

IV. 위수탁 업무 전반 개인정보보호 요건

앞서 소개한 개인정보 위수탁 업무 보안관리 프레임웍의 핵심 구성요소인 위수탁 업무 전반에 걸친 개인정보보호 요건들은 어떠한 내용으로 이루어져야 하는지 본 장에서 중점적으로 다루어 보고자 한다. 특히, 3.1.2절에서 언급한 바와 같이 개인정보 위수탁 업무 처리 과정을 '위수탁 업체 선정 및 계약' 단계, '위수탁 업무 진행' 단계, '위수탁 업무의 계약 해지 및 종료'의 3단계로 구분하고 각 과정별로 반드시 다루어져야 할 개인정보보호 요건들에 대하여 아래와 같이 상세히 언급하도록 한다.

4.1 "업체 선정 및 계약 단계" 시 고려사항

개인정보 위수탁에 따른 "업체 선정 및 계약 단계"에서는 개인정보보호법 및 개인정보보호표준지침에 명시된 바와 같은 "1)위탁목적 등의 문서화, 2)수탁업체 선정 기준 마련"의 법령 요건 이외에도 3)위수탁 업무이행 범위(Service Level Agreement: SLA) 검토와 4)위수탁 업무 관리 기준의 수립 등을 고려하여야 할 것이다.

4.1.1 위탁목적 등의 문서화

개인정보보호법 제26조제1항 및 동법 시행령 제28조제1항에 따라, 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다[3].

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 위탁업무의 목적 및 범위
4. 재위탁 제한에 관한 사항
5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
7. 수탁사가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

즉, 개인정보처리자는 개인정보 위수탁에 따른 계약 체결 시 상기에 명시된 바와 같은 사항들을 계약서 등에 반영하여 개인정보 위탁목적 등을 명확히 할 필요가 있다. 특히, 위 법령 요구사항 중 1. 위탁업무 수행목적에 필요한 개인정보의 처리 금지에 관한 사항과 3.위탁업무의 목적 및 범위 부분을 보다 명확히 하기 위하여 〔표3〕과 같이, 위탁되는 개인정보 유형 별 수집·이용 목적 분류표를 작성하여 최소한의 개인정보가 제3자에 의해 처리될 수 있도록 사전에 준비하는 것이 바람직할 것이다.

또한, 정보통신망법의 경우 정보통신서비스 제공자 등이 제3자에게 개인정보취급(수집・보관・처리・이

3) 개인정보 보호법령 및 지침·고시 해설서 190페이지

Table 3. Purpose of Collection/Use of Personal Information Classification Table

Type of Personal Information	Collection Route	Purpose of Collection	Mandatory /Optional
Name	Joining Membership	Identification of the person	Mandatory
Cellphone	Joining Membership	Customer Service	Mandatory
Home Address	Entering Shipping Address	Delivery of goods	Mandatory

용・제공・관리・폐기 등)업무를 위탁하여 처리할 경우, ①개인정보 취급을 위탁받는자(수탁사)와 ②개인정보 취급위탁의 업무내용에 대해 이용자에게 고지하고 동의를 얻어야 한다(법 제25조제1항).[4] 이에 따라, 위탁사는 해당 위탁업무를 처리함에 있어서 이용자(정보주체)에게 알리고 동의를 받기 위한 준비가 필요 할 것이다. 물론, 정보통신서비스 제공에 관한 계약의 이행을 위하여 필요한 경우에는 당해 위탁업무의 내용 및 수탁사를 이용자가 언제든지 확인할 수있도록 개인정보취급방침에 공개하거나, 전자우편・서면・모사전송・전화 또는 이와 유사한 방법으로 이용자에게 통지하는 것으로 이용자에게 동의를 얻어야하는 의무를 대신할 수는 있다.(법 제25조 제2항).

4.1.2 수탁업체 선정 기준 마련

개인정보보호표준지침 제19조 제1항에서는 개인정보처리자가 개인정보 처리 업무 수탁사를 선정할 때에는 수탁사의 "①인력, ②물적 시설, ③재정 부담능력, ④기술보유정도, ⑤책임능력"과 그 밖에 수탁사의 개인정보의 안전한 처리 및 처리를 위탁받은 개인정보의 보호와 관계되는 사항을 종합적으로 고려하여 선정하여야 한다고 명시하고 있다. 이 중 ①~⑤의 영역이 수탁사의 외형적인 규모를 고려한 사항이라면, 그 밖에 부분에서 언급하고 있는 '수탁사의 개인정보의 안전한 처리 및 처리를 위탁받은 개인정보의 보호와 관계되는 사항'의 영역을 수탁사의 개인정보보호를 위한 내부요소를 감안한 사항으로 판단하여 아래와 같은 수탁업체 선정 기준으로 고려할 수 있을 것으로 보인다. 즉, 수탁사 선정 단계에서부터 수탁업체의 개인정보보호와 관련한 의지 및 그간의 개인정보보호 수준 등에 대한 검토를 거쳐서 개인정보의 위수탁 과정에서 발생할 수 있는 위험요소를 사전에 줄이고자 하는 것이다.

✓ 외형적 규모
- 인력, 물적 시설, 재정 부담능력, 기술보유정도, 책임능력

✓ 개인정보보호 요소
- 사고여부, 전담인력·조직, 대외 인증 현황 등

물론, 수탁사의 재정적 능력을 초과하여 개인정보보호 의무를 과도하게 요구하는 부분을 최소화하기 위하여, 개인정보 위수탁 업무의 특성, 수탁사의 규모 및 위탁되는 개인정보의 유형 등을 종합적으로 고려하여 개인정보보호 요소를 수탁업체 선정 기준 중의 일부로 적용할 필요가 있을 것이다.

4.1.3 위수탁 업무이행 범위(SLA) 검토

개인정보를 위탁하는 과정에서 수탁업체와 반드시 협의해야 할 것 중의 하나가 개인정보 위수탁 업무 이행을 위한 SLA(Service Level Agreement)의 범위 선정이라고 할 수 있다. 이러한 SLA 범위를 선정하는 이유는 "1)위탁목적 등의 문서화"에서 명시한 위탁목적과 관련한 사항을 해당 개인정보 위탁업무에 맞게 보다 구체화하여 위탁된 개인정보의 안전한 처리와 보호를 보장하기 위함이다.

이러한 SLA 범위 선정의 지표로 개인정보보호표준지침 제19조제2항에서 언급된 "①수탁사의 처리업무의 지연, ②처리 업무와 관련 없는 불필요한 개인정보의 요구, ③처리기준의 불공정" 등의 문제점을 검토하여 활용할 수 있을 것이다. 이외에도, 위탁업무를 담당할 수탁사의 개인정보취급자 제한 방안, 수집·이용 목적 달성 시 파기 기한, 수탁사의 개인정보보호조치 활동과 관련한 보고 방안 및 방법 등을 종합적으로 고려하여 개인정보 위수탁에 따른 SLA 범위 선정 기준으로 활용할 수 있을 것이다.

특히, 위탁된 개인정보의 파기 및 수탁사의 개인정보보호조치 활동 등과 관련하여서는 향후 개인정보 유출 등으로 인해 야기할 수 있는 위·수탁사간 분쟁소지를 최소화하기 위하여 수탁사로서 준수해야 할 개인정보보호 요건에 따른 의무 이행 증적 제시 방안을 구체적으로 명시하는 것이 바람직할 것으로 보인다.

4) 정보통신서비스 제공자를 위한 개인정보보호 법령 해설서 41페이지

4.1.4 위수탁 업무 관리 기준 수립

개인정보 위수탁 업무 관리 기준은 엄밀히 말하자면, 개인정보처리자의 개인정보보호 관리체계라는 거시적 관점에서 접근하여 해당 개인정보처리자의 비즈니스 환경 및 업무목적에 부합하도록 수립하는 것이 바람직하다고 할 수 있다. 그럼에도 불구하고, 본 논문에서 제시하고자 하는 위수탁 업무 보안관리 프레임웍에서도 이러한 개인정보 위수탁 업무 관리 기준 부분은 반드시 짚고 넘어가야 할 사안이기에 아래와 같은 최소한의 고려사항을 제시하고자 한다.

- ✓ 수탁업체 관리 조직 및 유관부서 간(또는 담당자) 책임과 역할
- ✓ 수탁업체별 교육 기준 및 교육 컨텐츠 활용 방안 등 개인정보보호 교육 현황 관리 방안
- ✓ 수탁업체별 진단•감사 기준 및 수탁 업체 평가 기준 방안

4.2 "업무 진행 및 이행 단계" 항목

개인정보 위수탁에 따른 "업무 진행 및 이행 단계"에서는 개인정보보호법 및 동법 시행령에 따라 수탁사에 대한 교육 및 관리감독과 관련한 위탁사의 책임과 의무를 이행하여야 한다. 위탁사는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁사를 교육하고, 수탁사가 개인정보를 안전하게 처리하는지를 감독하여야 한다(개인정보보호법 제26조 제4항). 또한 위탁사는 수탁사가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위·수탁 계약의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다(동법 시행령 제28조제6항). 따라서 위탁사는 수탁사에 대하여 정기적인 교육을 실시하는 외에 수탁사의 개인정보처리 현황 및 실태, 목적외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.[5] 이러한 법령상 의무 이행 요건을 보다 효과적으로 이행하기 위해서 본 절에서는 1)수탁사 현황을 분류하고 관리 기준을 수립하는 방안과 더불어 이러한 관리 기준에 따라 2)수탁사 개인정보보호 수준 진단 및 평가체계를 운영하기 위한 방안을 제시하고자 한다.

4.2.1 수탁사 현황 분류 및 관리 기준 수립

개인정보 위탁업무에 따른 전체 수탁사별 현황을 분류하는 이유는 단순히 수탁업체의 목록을 관리하고 현황을 유지하기 위함이 아니라, 수탁업무의 특성, 수탁사의 규모와 제공되는 개인정보의 유형 등을 종합적으로 고려하여 위탁사 입장에서 보다 효율적으로 각각의 수탁사를 관리하기 위한 기준을 수립하는데 있다. 민병헌은 위탁업무에 따른 개인정보관리방안 연구[3]의 논문을 통해 개인정보 생명주기에 따른 위탁업무 현황을 분류[6]한 바 있다. 이 경우 각 위탁업무의 내용을 개인정보의 생명주기 즉, 수집, 저장, 이용·처리 및 파기 단계 별로 구분하여 수탁사 현황을 분류하였는데, 이러한 분류 과정을 이용한다면, 위탁사는 각 수탁사가 해당되는 개인정보 생명주기 유형 별로 필요한 개인정보보호조치를 보다 쉽게 가이드할 수 있으며, 수탁사 또한 수탁사 자신이 취해야 할 개인정보보호 활동에 대해 보다 명확하게 인지할 수 있는 이점이 존재할 수 있을 것이다.

본 논문에서는 이러한 수탁사 현황 분류 및 관리 기준 수립 시 고려해야 할 요소로 다음과 같은 항목들을 제시하고자 한다.

① 개인정보의 처리(제공)범위
- ✓ 수탁사의 물리적인 점유(완전 제공)
  - 콜센터, DM 및 배송업체 등
- ✓ 수탁사의 논리적인 점유
  - 전산 관리, 시스템 개발 등

② 개인정보의 유형 및 위탁 규모
- ✓ 일반신상정보, 금융정보, 고유식별정보, 민감정보 등 위탁되는 개인정보의 유형
- ✓ 연/월간 수탁사에 누적 제공되는 개인정보의 건수

③ 수탁사의 개인정보보호 수준
- ✓ 수탁사의 개인정보보호관련 조직/인원/예산 등 개인정보보호 관리 수준

5) 개인정보 보호법령 및 지침·고시 해설서 192페이지

6) 민병헌, 위탁업무에 따른 개인정보관리방안 연구, 15페이지

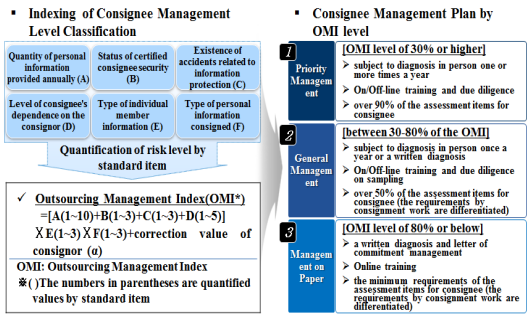

Fig. 4. Plan for Indexing of Consignee Management (example)

✓ 수탁사의 개인정보보호 사고유무, 개인정보보호 관련 인증 현황 등

④ 위탁업무의 일반성 및 특수성
✓ 실명확인, 본인인증, 금융거래 등 위탁사의 고유업무 이외 일반적인 위탁업무
✓ 매출 의존도가 높은 전속 수탁사 또는 위탁사의 고유업무 이행을 위한 특수 위탁업무

개인정보를 위탁받고 있는 전체 수탁사를 대상으로 이러한 기준으로 수탁사 현황을 분류한 후 ①~④에서 언급한 각각의 가중치를 부여하여 수탁사에 대한 관리 기준을 마련할 수 있을 것이다. 예를 들어, ①개인정보를 물리적으로 완전제공하고 있고, ②금융정보를 포함한 개인정보를 수탁하고 있으며, ③개인정보보호 관련 조직 및 인원이 없고, 사고 사례도 있으며 ④매출 의존도가 높은 전속 수탁사에 해당하는 경우, 위탁업무의 중요성 및 수탁업무의 특수성을 고려하여 해당 수탁사는 고위험군에 속하는 집중 관리 대상으로 분류하여 관리감독을 이행할 필요가 있다고 할 수 있다. 각 수탁사 현황 분류기준의 상세 유형 및 가중치의 경우 위탁업무의 특성을 고려하여야 할 것이나, 이러한 예에서 본 바와 같이 해당 수탁사 현황 분류기준을 토대로 개인정보보호 관련 유출 및 사고 위험 등을 고려하여 수치화 한다면, 수탁사별 현황 분류에 따른 고위험군 관리대상을 식별할 수 있을 것으로 보인다.

이러한 수탁사 관리 등급 분류를 위한 지수화 방안으로 ①~④에서 언급한 수탁사 관리 항목들과 위탁사의 가중치에 해당하는 보정값을 반영하여 〔그림 4〕의 예시와 같은 수탁사 관리 기준 지수(OMI[7])를 산정하고, 이러한 OMI지수에 따라 수탁사를 관리한다면, 보다 효율적이고 현실적인 수탁사 관리 기준을 수립할 수 있을 것이다. 즉, 〔그림4〕에서 보여지는 바와 같이, 각 수탁사별로 산출한 OMI 기준지수를 이용하여, OMI 기준 30% 이내, 30% ~ 80% 사이 및 80% 이하에 해당하는 각각의 수탁사를 중점관리, 일반관리 및 서면관리 그룹군으로 분류하고 각각 그룹군마다 수탁사 관리 및 평가 기준을 달리 적용할 수 있을 것이다.

4.2.2 수탁사 진단 및 평가체계 운영

수탁사별 개인정보 실태조사를 위한 진단 항목은 강태훈〔1〕, 이용진〔2〕의 연구성과에서도 살펴볼 수 있듯이 위탁업무의 특성을 고려하여 개인정보보호 관련 법령에 따라 마련할 수 있을 것으로 보인다. 수탁사 또한 위탁사와 동일하게 개인정보처리자로서의 법적 의무요건들을 이행해야 하기 때문에, 개인정보보호 관련 법규에서 규율하고 있는 법 조항 자체를 진단 항목으로 설정할 수도 있다. 강태훈〔1〕, 이용진〔2〕의 연구에서처럼 위탁업무 특성을 고려한 진단 항목을 개발하는 것도 의미가 있지만, 본 논문에서는 '1)수탁사 현황 분류 및 관리 기준 수립'에서 언급한 관리 기준에서 도출된 고위험군 여부에 따라 다음과 같은 수탁사 진단 기준 체계를 마련할 것을 권고하고자 한다.

또한, 이러한 수탁사 진단 기준에 따른 평가 이후 수탁사별 평가 체계를 위한 방안을 마련하는 것도 고려할 수 있다. 이러한 평가 체계와 관련해서는 강태훈〔1〕의 수탁사 진단 항목 위반 시 벌점을 부여하여 벌점별 제재를 부과하는 방안과 이용진〔2〕이 활용한 정보보호관리체계 수준평가 등급 기준〔8〕에 따라 수탁사에 대한 사전 보안등급 평가를 통해 수탁사에 대한 평가체계를 운영하는 방안 또한 고려할 수 있을 것이다.

① 수탁사 진단 방법 및 진단 주기
✓ 방문조사 / 서면조사 / 방문 후 서면조사
- 위탁사 자체조사, 외부 전문기관 참여 등
✓ 월 / 분기 / 반기 / 연 / 격년

② 수탁사 평가체계 운영
✓ 위반 시 벌점별 제재 기준 운영 및 상벌 적용
✓ 수탁사 보안등급 평가체계 운영

4.3 "계약 해지 및 종료 단계" 항목

7) OMI: Outsourcing Management Index

개인정보의 위수탁 업무 목적을 달성하여 더 이상 해당 업무를 위한 개인정보를 제3자에게 위탁할 필요가 없어지거나, 수탁사의 교체로 인하여 이전 수탁사와의 계약을 해지하는 경우, 즉 위수탁 업무의 계약 해지 및 종료 단계에서 고려하여야 할 사항에 대하여 살펴보고자 한다.

현행 법령상 계약의 해지 및 종료 단계에서 위탁사의 책임과 의무에 관해서는 앞에서도 언급한 바와 같이 개인정보보호법 제26조 제4항에 따라 수탁사가 개인정보를 안전하게 처리하는지를 감독하여야 한다고 규율하고 있으나, 관련하여 구체적인 내용을 언급하고 있지는 않다.

이에 본 논문에서는 위수탁 업무의 계약 해지 및 종료라는 단계에서 고려해야 할 요소로 개인정보의 수집·이용 목적 달성이라는 점을 감안하여 1)개인정보를 안전하게 파기하였음을 확인하는 것과 수탁사가 수탁 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하는 등의 불법행위를 자행하지 않았음을 보증하기 위한 2)사후관리 보증을 위한 대책을 마련할 것을 제안하고자 한다.

① 개인정보 파기 및 회수 확인
- ✓ 파기 확인서 징구 및 증적 보관
- ✓ 재생 및 복구 불가능한 방식 적용
- ✓ 샘플링 점검을 통한 파기 및 회수 검증

② 사후관리 보증 방안 마련
- ✓ 개인정보보호 법규 준수 확인 및 보안서약
- ✓ 목적외 이용 등 부정 사용 건에 대한 배상 및 책임 체계 마련
- ✓ 신의성실원칙에 의한 위탁업무 이관

V. 결 론

지금까지 본 논문에서는 개인정보의 위수탁 업무 처리 과정을 '업체 선정 및 계약' 단계, '업무 진행 및 이행' 단계, '계약 해지 및 종료'의 3단계로 구분하고 각 과정별로 반드시 다루어져야 할 개인정보보호 요건들에 대하여 언급하였다. 전술한 바와 같이, 첫 번째, '업체 선정 및 계약' 단계에서는 위탁 목적을 문서화하고, 수탁사 선정 시 고려 요건들을 명확히 하여 수탁사를 통해 발생할 수 있는 위험요소들을 사전에 식별하고 이를 완화하고자 하였으며, 계약 시 법적 의무 요건 뿐만 아니라, 위탁업무 이행 SLA를 검토하고 이를 계약 사항에 반영할 것을 권고하였다.

또한, 두 번째, '업무 진행 및 이행' 단계에서는 기존의 연구 성과들이 주로 수탁사가 준수해야할 점검항목들을 중심으로 수탁사의 업무 특성을 고려한 개인정보보호 의무 이행 요건들을 도출하고 이를 실제 적용하는 관점으로 진행된 점을 감안하여, 본 논문에서는 이러한 '업무 진행 및 이행' 단계에서 수탁사 관리를 위한 점검항목 항목 도출과 더불어, 위탁사가 보다 효율적이고 실질적인 수탁사 관리를 수행할 수 있도록 수탁사 관리지수를 통한 수탁사 관리 등급을 분류하는 방안을 제시하였다.

세 번째, '계약 해지 및 종료' 단계에서는 개인정보의 파기 및 회수와 더불어 개인정보 처리 업무의 사후적 쟁점 및 이슈요건들을 완화하기 위한 보증 방안을 마련할 것을 언급하였다. 뿐만 아니라, 이러한 개인정보 처리 위탁 업무 전 과정에서의 수탁사 관리 기준과 위탁사가 기존에 개인정보처리자로서 행하고 있는 개인정보보호 관리체계와의 연계 방안들을 종합한 위수탁 업무 개인정보 보안관리 프레임웍을 제안하고자 하였다.

이와같이 본 논문에서 제안하는 바가 개인정보 위수탁 업무의 다양성, 개인정보의 처리를 위탁하는 위탁사 및 위탁받는 수탁사의 비즈니스 환경, 업체 규모 등의 현실적인 요소들과 접목되어 개인정보의 위수탁 업무 과정에서 발생가능한 다양한 보안위험을 줄이고 이를 통해 실질적으로 수탁사에 대한 보안관리를 강화하여 개인정보 유출 등의 사건·사고를 미연에 예방하는데 조금이나마 기여할 수 있었으면 하는 바람이다.

References

〔1〕 Taehoon Kang, Jongin Yim, Study on Measures to Strengthen Personal Information Protection Consignee Management System, VOL.23, NO.4, 2013, 8, Journal of the Korea Institute of Information Security and Cryptology, pp. 781-797.

〔2〕 Yongjin Lee, Jongin Yim, Study on the Status of Supervision on Management of Financial Company's Personal Credit Information Consignee and Ways of Improvements , Journal of Security

Engineering, Vol.11, No.3 (2014), pp.233-250.
〔3〕 Byunghyun Min, Study on Personal Information Management Plan for Consignment Work, 2014, A Master's Thesis for Graduate School of Information and Communication, Sungkyunkwan University
〔4〕 Ministry of Government Legislation, http://www.law.go.kr, Personal Information Protection Act
〔5〕 Ministry of Government Legislation, http://www.law.go.kr, Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.
〔6〕 Ministry of Government Legislation, http://www.law.go.kr, Electronic Financial Transactions Act
〔7〕 Ministry of Government Legislation, http://www.law.go.kr, Use and Protection of Credit Information Act
〔8〕 Korea Internet & Security Agency, "Study on Assessment Methodology of Information Protection Management System Level and Standards of Level", 2010, 9
〔9〕 The Payment Card Industry Security Standards Counsil, Payment Card Industry (PCI) Data Security Standard, Oct (2010).
〔10〕 http://sharedassessments.org/about/, Jan (2012).
〔11〕 NIA(National Information Society Agency), 2012 The first half year of Trend for Oversea Policy Privacy Security, Jun (2012).
〔12〕 Notification of Korea Communication Commission No. 2015-2, 2015. 1. 13

〈저자소개〉

고 영 대 (Young-dai Ko) 정회원
2002년 8월: 서울시립대학교 수학과 졸업
2004년 8월: 고려대학교 정보보호대학원 정보보호학과 석사
2013년 3월~2015년 2월: 고려대학교 정보보호대학원 정보보호학과 박사 수료
2013년 2월~현재: 법무법인(유) 율촌 전문위원
〈관심분야〉 개인정보보호, 정보보호, 디지털 포렌식, 대칭키 암호

이 상 진 (Sang-jin Lee) 종신회원
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 대칭키 암호, 정보은닉이론, 디지털 포렌식