KIPS Trans. Comp. and Comm. Sys.
Vol.12, No.11 pp.329~336
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2023.12.11.329

Research on Framework and Inspection Method to Strengthen Personal Information Protection of Trustees

Yurim Bak† · Yongtae Shin††

ABSTRACT

This paper analyzes the Personal Information Protection Act and related legal guides revised in 2023, proposes a framework for a consignment contract through the items necessary in the consignment relationship for personal information work, and inspects the status of personal information protection for consignees that are absent in Korea. By proposing common items that must be included, we prevent the occurrence of personal information leakage incidents by strengthening the basic personal information protection capabilities of trustees handling personal information work and alleviating the burden of essential personal information protection inspections. I want to do it.

Keywords : Privacy, Framework, Check List, Consinging, Re-Consigning

수탁사 개인정보보호 강화를 위한 프레임워크 및 점검방법 연구

박 유 림† · 신 용 태††

요 약

본 논문은 2023년 개정된 개인정보보호법 및 관련 법적 가이드 등을 분석하고, 개인정보 업무 위수탁 관계에서 필요한 항목을 통해 위수탁 계약에 대한 프레임워크를 제안하고, 국내에 부재한 수탁사 개인정보보호 현황 점검의 필수적으로 포함되어야 하는 공통항목을 제안함으로서, 개인정보 업무를 처리하는 수탁사의 기본적인 개인정보보호 역량의 강화와 필수적으로 수행하는 개인정보보호 점검에 대한 부담감을 완화하고 개인정보 유출 사고 발생 예방에 기여하고자 한다.

키워드 : 개인정보보호, 프레임워크, 점검항목, 업무 위탁, 재수탁

1. 서 론

개인정보는 데이터 3법 개정, 기술의 발전, 사용자의 요구에 따라 다방면의 서비스에 활용되고 있다. 이러한 활용률의 증가에 따라 정보주체의 권리 보장 및 안전한 개인정보 운용이 요구되었으며, 개인정보보호법 개정과 관련 가이드 등을 통해 보안 수준을 향상시키도록 하고 있다. 다만, 개인정보보호법 개정으로 보안성 향상을 기대할 수 있으나, 작은 규모의 영세기업은 모든 법을 준수하기에 현실적으로 어려운 상황이다. 간단한 예시로 개인정보보호법 제29조(안전조치의무)에서는 접속기록을 보관해야 한다고 명시하고 있지만, 개인정보처리 시스템을 구축이 어려운 영세기업은 해당 법을 준수하기 어렵다. 대다수의 영세기업은 상대적으로 큰 규모의 기업으로부터 특정 업무를 위탁받아 업무를 처리하거나, 시스템을 이용하여 업무를 처리하는 구조가 많다. 개인정보를 처리해야 하는 부분에서 개인정보보호를 위한 조치는 많은 투자와 업무 부담이 발생한다. 이외에도 업무를 위탁하는 기업들은 서비스 제공에 전문적인 영역을 직접 수행하기보다는 전문 기업에 업무를 위탁하는 형태로 운영된다. 이 과정에서 다양한 유형의 개인정보가 위탁업체로 제공되고, 처리되고, 폐기된다. 즉, 현재의 기업환경에서 개인정보의 생명주기는 하나의 기업이 아닌 다수의 기업에서 순환되고 있는 것이다. 문제는 업무를 위탁받은 위탁사에 대한 개인정보보호 수준을 관리하는 부분이다[1].

개인정보 위수탁에 대해서 개인정보보호법의 개정, 가이드 등이 제작되어 법을 준수하도록 도움을 주고 있지만, 개인정보 위탁사를 위한 가이드는 지속적인 개정이 이루어지지 않고, 점검 항목이 빈약하여 실효성이 부족하다[2]. 이러한 환경에서 개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리제한) 내용에 따라 수탁사의 개인정보 관리 미숙에 따른 피해를 위탁사가 책임져야 하는 상황으로 인해 위탁사는 정기적으로 수탁사에 대한 개인정보보호 점검을 수행한다. 다만, 점검 항목에 대한 명확한 표준이나 기준이 부재함에 따라 개인정보보호 점검의 수준은 위탁사의 의지에 따라 차이가 발생한

† 정 회 원 : 한국국방연구원 국방데이터분석센터 연구원
†† 종신회원 : 숭실대학교 컴퓨터공학보 교수
Manuscript Received : October 5, 2023
Accepted : October 27, 2023
* Corresponding Author : Yongtae Shin(shin@ssu.ac.kr)

다는 문제점이 있다. 또한, 2023년에 개정된 개인정보보호법은 수탁사의 재수탁에 대하여 위탁사의 동의가 필수 요소 변경되었고, 이에 따라 재수탁사에 대한 관리도 기존 수탁사와 동일하게 관리해야 하는 상황이 되었다.

개인정보 피해를 예방하기 위한 법령 개정의 목적이 가이드의 부재로 인해 사각이 발생하고, 법령 개정에 대한 효과성이 상실되고 있다[2]. 모든 분야에 적용할 수 있는 가이드를 만드는 것은 어렵지만, 공통적인 부분과 필수사항 등에 대해서는 반드시 법적 효력을 갖춘 가이드라인이 제정될 필요가 있다[3].

본 논문에서는 개인정보 업무 수탁사에 대한 점검 가이드 부재 문제점에 대하여 점검의 필수적인 공통사항을 도출하고, 위수탁 관계에서 준수하여야 하는 통제항목 및 관리 기준 등을 제안한다. 해당 기준은 현실적인 상황을 반영하여 계약된 위탁사와 수탁사의 규모 등을 고려하도록 한다.

2. 관련 연구

2.1 개인정보 생명주기

개인정보 생명주기는 4단계로 구성(수집-보유·이용-제공-파기)된다. 또한 각 단계별로 법적준수사항으로 세부구성이 되어 있다.

개인정보를 보호한다는 것은 생명주기를 기본으로 구분하여 각 단계별로 관리적, 물리적, 기술적 관점으로 방안을 마련하여야 한다. 이러한 대표적인 프레임워크가 ISMS-P 인증이다[4].

ISMS-P는 과거 ISMS와 PIMS가 통합되며 등장한 인증으로

Table 1. Life-Cycle of Personal Information

Collect	- Personal Information Collection and Usage Agreement - Restrictions on collection of personal information - Consent of legal representative for children under 14 years of age - Restriction on processing sensitive and unique identity information of personal information - Providing identity verification methods other than resident registration number
Use	- Disclosure of Privacy Policy - Appointment of personal information protection officer - Measures to ensure personal information safety
Provide	- Consent to provision of personal information to third parties - Prohibition of use of personal information for purposes other than purposes - Personal information processing entrustment, business transfer, transfer, etc.
Destruct	- Destruction upon expiration of retention period - Destruction process

근간은 ISO27001에 두고 있다. 정보보호 측면의 ISMS와 개인정보 측면의 PIMS를 관리적, 물리적, 기술적 분야로 평가함으로서 종합적인 보호수준을 산정한다. 이렇듯 개인정보는 생명주기를 기준으로 분류되고, 개인정보 위수탁 업무는 수집부터 시작하는 경우도 존재하나, 대다수는 제공이라는 단계에서 수행된다[5].

개인정보 위탁 업무의 대다수가 제공단계라고 하더라도, 업무를 위탁받은 수탁사는 제공받은 개인정보를 관리하여야 하므로 보유·이용 단계부터 보호조치를 수행하여야 한다[6].

2.2 개인정보보호법 개정[7]

개인정보보호법은 2011년 재정 이후 기업의 생태 변화에 맞춰 2023년까지 지속적으로 개정되었다. 현재 개정된 개인정보보호법의 주요 개정사항은 영상정보처리의 고정형과 이동형의 분리, 개인정보 영향평가 결과 공개, 개인정보 업무 수탁자의 재수탁시 위탁사의 동의, 처벌규정 강화 등이 있다.

영상정보처리기기는 고정되어 촬영하는 CCTV와 같은 고정형 영상정보처리기기와 스마트폰 카메라, 드론 등 이동하며 촬영하는 이동형 영상정보처리기기로 구분되어 법적 적용 사항을 달리하고 있다. 미디어 플랫폼의 활성화로 인해 일반인의 미디어 콘텐츠 제작이 활발함에 따라 개정된 사항이다. 개인정보 영향 평가 수행을 확대하는 내용으로 영향 평가 수행 시점을 명확히 하고, 영향평가서를 요약하여 공개하는 내용이다. 본 논문과 연관된 개정 내용은 개인정보 업무 수탁자가 업무의 일부를 다른 기업에 재위탁할 경우에 위탁자의 동의를 받아야 한다는 내용으로 재수탁시 위탁사의 동의가 반드시 필요하다는 내용이다.

위수탁 관계에서 재수탁에 대한 부분도 위탁사가 관리하도록 하는 내용으로 개인정보 침해 사고를 예방하기 위한 차원으로 해당 내용이 신설됨에 따라 과거 수탁사에 대해서만 요구되던 개인정보 보호 수준이 재수탁사 까지 확대 적용되어야 함을 의미하고 있다.

2.3 개인정보 업무 위수탁 점검 가이드

국내에 제정된 개인정보 위수탁 점검에 참고할 수 있는 가이드는 2020년에 개인정보보호 위원회에서 발간한 개인정보처리 위·수탁 안내서가 전부다[8]. 해당 가이드는 개인정보보호법을 기반으로 위수탁 단계별 조치사항에 대한 자세한 내용을 사례로 쉽게 이해할 수 있도록 안내하고 있다. 수탁사를 선택하기 앞서 제공되는 개인정보에 대한 위험성 평가, 수탁사에 대한 개인정보 보호 역량 분석, 위수탁 계약 관계에서 필수적으로 포함되어야 하는 내용 6가지, 수탁사에 대한 교육 수행, 재위탁시 준수사항 등이 주요 내용이다. 즉, 위탁자와 수탁자의 관계에 대한 내용이 중심인 가이드이고, 개인정보보호법에 따른 수탁사 관리를 위한 점검 내용은 하나의 체크리스트로 제공하고 있다.

제공되는 체크리스트는 3단계의 위수탁 단계별로 13개의 점검항목으로 구성되어 있으며 각 항목별로 대상이 구분되어 있다. 수탁사의 개인정보보호 역량 평가 및 개인정보보호법 준수 가능성을 판단하기 위해서는 관리적, 물리적, 기술적 관점에서 상세하게 점검이 이루어져야 하는 현실에는 도움이 되지 못하는 가이드이다. 이외에도 개인정보보호법이 개정됨에 따라 지속적으로 갱신되지 못하는 문제도 갖고 있다.

수탁사의 개인정보보호 역량을 평가하기 위해서는 위수탁 점검 가이드보다 2020년에 발간한 개인정보의 안전성 확보조치 기준 해설서가 더욱 적합하다. 해당 해설서가 수탁사를 대상으로 작성된 것은 아니지만, 개인정보를 다루는 주체가 준수해야하는 항목들을 제공하고 있다. 개인정보보호법을 기반으로 제23조, 제24조, 제29조 등의 법령을 해설하여 준수할 수 있도록 안내하는 것을 목적으로 하고 있다. 관리적, 물리적, 기술적 측면으로 개인정보를 안전하게 관리하기 위한 방안을 설명하고 있으며, 조-항-호의 구조로 63개 항목에 대한 체크리스트를 제공하고 있다. 다만, 해당 내용이 위수탁 관계에서 점검을 위한 용도가 아님에 따라 모든 기업이 해당 내용을 준수하기에는 현실적인 어려움이 있다. 또한, 해당 해설서도 개인정보보호법 개정에 따라 지속적으로 갱신되지 못하는 문제를 갖고 있다.

이런 환경에서 위탁사는 수탁사의 개인정보 관리 미흡으로 인한 피해발생을 최소화 하기 위해 자체적으로 수탁사에 대한 점검을 수행하여야 하는데, 기업의 규모와 상관없이 필수적이고, 공통으로 적용할 수 있는 명확한 지표가 부재하여 점검을 수행함에 어려움을 겪고 있다. 또한, 위탁사가 자체적으로 개인정보보호법을 기반으로 각자의 점검항목을 구성하고 점검을 수행하는 것은 국내 기업의 개인정보보호 수준의 역량을 향상시킬 수도 있지만, 반대로 저하시킬 위험성을 갖을 수도 있다[9].

3. 수탁사 개인정보보호 점검

개인정보 관련 업무 위탁은 수탁사의 개인정보보호 역량이 중요하지만, 이를 관리 감독하는 위탁사의 역할 또한 중요하다. 본 장에서는 개인정보 업무 위수탁에 대한 프레임워크와 수탁사를 점검하기 위한 필수사항을 정의하여 앞서 도출한 위수탁 관계에서의 문제점을 해소하고 한다.

3.1 행위주체 정의

본 논문은 혼동하기 쉬운 행위 주체들이 등장함에 따라 제안 내용을 진행하기 앞서 용어에 대한 정의를 설명한다.

1) 위탁사 : 개인정보를 보유하고 있는 주체이며, 개인정보 업무를 위탁 주는 대상
2) 수탁사 : 개인정보를 제공받는 주체이며, 개인정보 업무를 위탁 받아 수행하는 대상
3) 재수탁사 : 수탁사가 처리해야하는 개인정보 업무 일부를 위탁 받아 수행하는 대상

Table 2. Framework of Consigning of Personal Information

Contract	- Definition of entrusted work - Entrusted personal information list - Method of provision and protection of personal information - Proceed with a re-consignment contract with the consent of the original consignor
Implementation	- Perform contracted work - (Trustee)Personal information protection and management - (Consignor)Personal information protection status management - (Consignor)Management of personal information protection status of re-trustee
End	- Destruction of personal information

3.2 개인정보 업무 위탁사 관리 프레임워크

제안하는 개인정보 업무 위탁 관리 프레임워크는 계약, 이행, 종료의 3단계로 구분되며 각 단계별로 세부 요구사항으로 구성했다.

계약 단계에서는 위탁하는 업무에 대한 명확한 정의를 수행한다. 계약하는 업무 분야에 따라 적용되는 법적 사항은 다르고, 이를 준수하기 위한 방안이 다를 수 있다. 다만, 수탁사에 제공되는 개인정보 항목은 개인정보처리 방침과 유사하게 필요한 업무를 정의하고, 요구되는 개인정보 항목과 보유기간을 명시함으로써 불필요한 정보 활용을 예방할 수 있도록 한다. 이는 개인정보보호법에 명시된 목적 외의 용도 활용을 사전에 예방하기 위해서다. 제공되는 개인정보 항목은 위탁사의 개인정보처리방침에 보유기간을 기준으로 보유하게 되며, 활용 시 활용내역을 저장·관리하도록 한다. 개인정보 보호 방안은 개인정보보호법에 명시된 내용을 준수하여 보호하고, 본 논문에서 제안하는 점검 항목을 기반으로 한다.

수탁사가 재수탁을 진행할 경우, 개정된 개인정보보호법에 따라 사전에 위탁사의 동의를 받아야 하며, 위탁사는 재수탁사에 대한 개인정보보호 역량 진단 수행을 의무화한다. 의무화 방안은 계약된 수탁사는 위탁사가 요구하는 개인정보보호 수준을 만족한다는 전제하에 계약이 진행된 것으로 재수탁사도 이에 준하는 개인정보보호 수준을 갖추어야 한다.

이행 단계에서는 계약 이후, 위탁받은 업무를 수행하는 단계로 사전에 합의된 인원을 대상으로 개인정보 접근권한 할당 및 이용 이력을 관리하도록 한다. 업무에 이용되는 시스템, 단말기, 보조 저장장치, 이동형 저장매체 등도 사전에 위탁사 승인하에 활용될 수 있도록 한다. 이는 비인가된 시스템, 단말기 등의 이용과정에서 외부의 악의적인 공격을 사전에 차단할 수 있도록 조치하고, 이후 종료 단계에서 개인정보를 명확하게 파기하기 위해 필요한 조치다. 인가된 시스템, 단말기만을 사용함으로써 기술적인 보호 조치를 사전에 정의할 수 있고, 개인정보보호 법령에 따른 위탁사의 관리가 현실적으로 가능하게 하기 위함이다. 수탁사에서 추가적인 시스템 이용, 단말기 증축 등은 위탁사에게 재승인 요청 과정을 추가하여 진행할

수 있도록 하고, 위탁사는 추가적인 대상에 대한 보호 조치를 점검할 수 있도록 한다.

수탁사는 계약된 업무를 위해 제공받은 개인정보를 기술적 보호 조치로 외부의 위협으로부터 안전하게 관리할 수 있도록 한다. 위탁사는 수탁사에서 개인정보를 안전하게 관리할 수 있도록 제안하는 체크리스트를 기반으로 이행단계에서 연 1회 이상 보안점검을 수행하고, 월별 활동에 대한 증적을 위탁사에 제공한다. 이를 통해 취약한 항목은 보완조치를 수행할 수 있도록 한고, 계약 단계에서 협의된 내용이 정상적으로 이행되는지 점검할 수 있도록 한다. 개인정보보호법은 수탁사의 개인정보 피해를 위탁사가 책임지도록 정의함에 따라, 개인정보보호를 정상적으로 수행하지 않는 수탁사들도 존재한다. 이러한 행위는 잠재적인 위험을 내포하고 있으며, 발생되는 피해는 위탁사 뿐만 아니라 정보주체까지 영향을 끼친다. 따라서 일방적인 위탁사의 수탁사 점검 방법이 아닌 월별 활동에 대하 증적을 수탁사에서 직접 수행하도록 함으로서 상호 관리에 대한 방안을 마련하고, 위탁 업무에 대한 신뢰성과 안전성을 확보할 수 있도록 한다. 재수탁사가 존재하는 경우, 위탁사가 직접 재수탁사에 대한 개인정보보호 점검을 수행하고, 수탁사를 통해 보완조치를 요구할 수 있도록 한다. 이는 앞서 말한 것처럼 위탁사의 개인정보보호 수준을 확보하기 위함이다.

종료 단계는 계약된 기간이 종료됨에 따라 개인정보를 처리해야 하는 단계이다. 위탁받은 업무에 따라 수집 혹은 제공받은 개인정보를 파기하는 단계로서 이행 단계에서 승인된 시스템, 단말기, 보조 저장장치, 이동형 저장매체 등을 대상으로 완전 삭제 등의 조치가 수행된다. 파기는 제공받은 개인정보 형태에 따라 다르게 수행된다. 전자파일로 제공된 개인정보는 복구가 불가능한 삭제 방식으로 수행하고, 문서 형태는 세절기 등을 통해 파기를 수행한다. 만약 이 과정에서 단말기, 저장매체 등에 대한 파기를 수행하는 경우에는 재사용이 불가능한 방식을 적용한다.

위탁사와 수탁사 계약관계에서 파기가 아닌 정보 이전내용이 포함되어 있다면, 수집된 개인정보를 위탁사로 이전하고, 파기를 수행한다, 모든 파기는 파기확인서를 작성하고 위탁사에 전달함으로서 업무를 종료하도록 한다.

3.3 수탁사 개인정보보호 필수 점검항목

수탁사의 개인정보보호 현황을 점검하기 위한 구체적인 항목은 현재 마련되어 있지 않다. 개인정보를 다루는 기업을 대상으로만 가이드가 마련되어 있지만, 수탁사에 모두 적용하기도 현실적으로 어려움이 존재한다. 또한, 개인정보 처리 업무 분야에 따라 보호 방안 등이 다르게 적용되어야 한다. 하지만, 수탁사를 위한 개인정보보호 점검은 공통 적용할 수 있는 기준을 통해 점검해야만 모든 대상에 명확한 현황을 파악할 수 있다. 따라서 수탁사 개인정보보호 점검을 위한 공통사항을 도출하고, 현실적으로 준수할 수 있는 점검 항목을 제안하고자 한다. 점검 항목은 관리적, 물리적, 기술적, 생명주기 측면, 재수탁 측면으로 구성되어 있다.

Table 3. Check List of Management Focus

Management	- Privacy policy document for consignment work - Personal information protection organization - Management of personal information handler - Request for security pledge from personal information hadler or CEO - Application for prior consent for personal information access device and system

1) 관리적 측면

관리적 측면은 정책, 조직, 취급자 관리로 구성되어 있다.

개인정보보호 정책은 기업 내 위탁받은 업무 및 제공받는 개인정보에 대한 보호 계획 및 규정 등을 정의한 문서로서 연 1회 이상 정기적으로 점검되어야 하고, 이사회 또는 대표이사가 직접 승인한 문서를 의미한다. 이렇듯 전사적인 측면의 문서로 개인정보에 대한 모든 내용을 내포하고 있게 된다. 이는 위탁받은 업무와 연관이 없는 부분도 존재할 수 있고, 보호하기 위한 방안이 부재할 수 있다는 것을 의미한다. 따라서 기존의 기업용 정책문서가 아닌, 업무를 위탁받은 업무 범위로 한정하여 개인정보 관리 및 보호 관련 내용을 포함하도록 한다. 이를 통해 정확한 업무환경, 보호방안 등 실현가능한 형태로 작성될 것이다. 또한, 정기적인 검토가 원활하게 이루어질 수 있다.

개인정보보호 조직은 제공받은 개인정보를 처리·관리하는 담당자의 지정 여부를 확인하는 것으로 기업 내 지정된 개인정보보호 책임자가 아닌, 위탁 업무에 한하여 개인정보 담당자를 지정하는 것이다. 영세기업의 경우 개인정보보호 책임자가 겸업을 할 수 있고, 위탁 업무 계약이 많은 수탁사의 정보보호 책임자는 모든 개인정보를 관리하기 어려울 수 있다. 따라서 개인정보 담당자를 지정하여 영세기업은 위탁 업무 담당자로 관리의 용이성을 확보하고, 위탁 업무 계약이 많은 수탁사는 담당자와 책임자간의 유기적인 관계를 통해 안전하게 관리될 수 있도록 한다.

개인정보 취급자 관리는 보안서약서를 징구하고, 정기적으로 교육을 이수한다. 다만, 개인정보 취급자가 별도로 정해지지 않은 업무일 경우에는 대표의 보안서약서 징구로 대체한다. 개인정보 취급자가 명확하게 지정할 수 없는 배송과 같은 업무의 경우, 모든 임직원에게 보안서약서를 징구하는 것은 사실상 불가능하다. 따라서 대표의 보안서약서 징구를 통해 수탁사가 거버넌스 측면으로 개인정보를 보호하고 책임질 수 있음을 증명하도록 한다. 또한, 사전에 승인된 시스템 및 단말기만을 사용하도록 함으로서 개인정보의 관리 및 보안 측면의 용이성을 확보하도록 한다. 이는 보안성 확보가 상대적으로 유리하고, 개인정보 유출에 따른 추적, 업무 종료에 따른 파기 등으로 높은 안정성을 확보할 수 있다.

2) 물리적 측면

물리적 측면은 외부인 출입통제, 개인정보 접근통제, 저장매체 보안 등으로 구성되어 있다.

Table 4. Check List of Physical Focus

Physical	- Separation of work areas (control access of outsiders if necessary) - Personal information access control - Storage media security

업무영역 분리는 사무실 내 출입이 아닌, 위탁 업무에 대한 취급자의 업무영역 분리를 의미하며, 별도의 공간이 마련되어 있는 경우는 출입통제로 적용한다. 기업 내 혹은 사무실 내 출입통제는 위탁 업무와 연관이 적은 방문자 또한 관리 대상이 되는 불필요한 관리로 확대될 수 있기에 통제 부분을 업무영역의 분리로 변경될 필요가 있다. 업무영역의 분리를 물리적으로 공간을 독립하는 것이 바람직하나, 기업의 규모에 따라 현실성이 낮은 방향이다. 따라서 물리적인 사무실 분리가 아닌, 업무영역에 따른 권한, 단말기 접근통제 등의 방식으로 분리를 수행한다.

개인정보 접근통제는 제공받은 개인정보에 대한 비인가자의 접근을 방지하는 것을 의미한다. 개인정보 형태에 따라 전자적 파일인 경우 단말기에 대한 접근을 통제하고, 물리적 형태는 시건장치 등이 된 장소에 보관하도록 한다.

저장매체 보안은 이동형 저장매체 및 노트북 등에 대한 보안으로 해당 개인정보를 DRM 혹은 암호화를 하거나, 이동이 잦을 경우에는 보안 USB 사용을 의미한다.

3) 기술적 측면

기술적 측면은 전자파일 형태의 개인정보를 IT 기술을 적용하여 안전하게 관리하는 것을 의미한다. 접근권한 관리, 접속기록 관리, 비밀번호 관리, DB 암호화, 서버 및 네트워크 접근제어, 단말기 보안성 확보 등으로 구성된다.

기술적 측면은 ISMS-P의 개인정보 통제항목 및 개인정보보호법을 근간으로 구성함에 따라 주요 특징적인 부분에 대해서만 설명한다. 제공받은 개인정보를 안전하게 보호하기 위한 암호화, 접근제어, 단말기 보안 등은 개인정보보호 준수사항과 동일하게 적용하므로 생략한다. 기존의 방식과 차이점은 접근권한 관리 이력, 접속기록 관리 이력 부분의 보관 주체이다. 기존의 방식으로 수탁사에 대한 보호 방안을 해석해보면 접근권한 관리 이력 및 접속기록 관리 이력 등은 수탁사에서 보관·관리하는 것으로 볼 수 있다. 또한, 월 1회 이상 점검을 수행하도록 되어있다. 제안하는 방식은 위탁사에서 직접 관리하고, 점검을 수행하여 취약사항을 최소화하는 것으로 이는 악의적인 이용자에 의해 내용이 변경될 위험성이 존재하며,

Table 5. Check List of Technical Focus

Techinical	- Access authority management history - Access record management history - Password management - DB encryption - Server and network access control - Personal information access device security

Table 6. Check List of Personal Information Life-Cycle Focus

Personal information Life-Cycle	- Establishment of Privacy Policy - Agreement of Personal information collection and consent - Personal information masking - Destruction of personal information

수탁사에 대한 개인정보 관리 측면에서도 위탁사가 수행하는 것이 바람직하다.

4) 생명주기 측면

생명주기 측면은 개인정보의 생명주기에 따른 보호 방안을 점검하는 것으로 개인정보처리 방침 수립, 수집, 마스킹, 파기 등으로 구성한다.

생명주기 측면은 위탁받은 업무 내에 개인정보 수집의 포함 여부에 따라 적용이 달라진다. 해당 내용은 개인정보보호법 및 관련 법적 가이드로 해설되어 있는 내용과 동일하므로 생략한다.

5) 재수탁 측면

재수탁 측면은 2023년 개정된 개인정보보호법을 고려하여 항목을 구성하였으며, 기업들 대다수가 영향을 받는 부분이다.

2023년 개정된 개인정보보호법은 수탁사가 또 다른 수탁사와 계약할 때에 위탁사에 승인을 받아야 한다고 명시하고 있다. 즉, 재수탁사와 계약 시 보안 현황을 확인하고, 지속적으로 관리를 수행하여야 한다는 의미다. 재수탁사에 대한 개인정보보호 점검은 현실적으로 어려운 부분이 많다. 가령 수탁사인 영세사업자가 물류 배송을 위해 대기업 배송업체와 재수탁 계약을 체결한 경우 개인정보보호 점검을 현 위탁사와 수탁사 관계를 기준으로 수행이 불가능하다. 하나의 예시로 현행 체계에서는 위탁사는 수탁사에게 개인정보보호 교육을 연 1회 이상 수행하여야 하고, 개인정보 현황 점검을 수행하여야 한다고 명시되어 있지만, 영세사업자가 대기업을 대상으

Table 7. Check List of Re-entrustment Focus

Re-entrustment	- The original consignor's signature is included in the consignment contract. - Preparation of policy documents for protection of re-trusted work and provided personal information - Providing the status of regular personal information protection inspections by the subtrustee itself or the consignor - Management of original consignor's personal information access authority and access record history - Request for security pledge from personal information hadler or CEO - Presentation of certificate of completion of personal information protection training for executives and employees of subcontractor - Prior consent for personal information access devices and systems

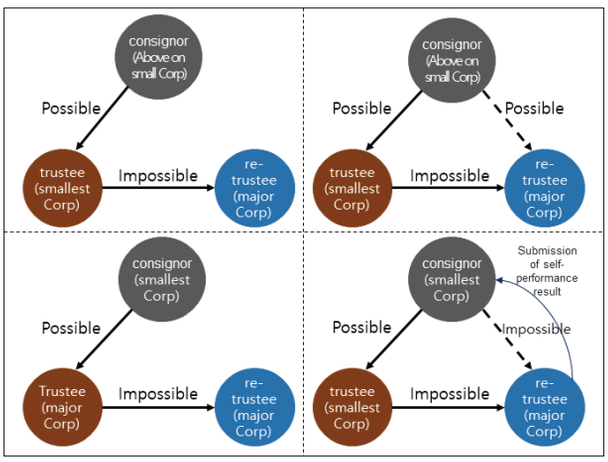

Fig. 1. Consignment Relationship Depending on Company Size

로 교육 수행을 어려울 뿐만 아니라, 개인정보 현황을 점검하는 부분도 불가능할 것이다. 대기업의 물류 배송담당자 모두에게 보안서약서를 징구하는 것도 불가하다. 따라서 재수탁에 대해서는 기존의 위탁사와 수탁사 관계가 아닌 현실적으로 점검이 가능한 재수탁 측면을 구성하여 위탁사-수탁사-재수탁사 간의 이해관계를 명확하게 할 필요가 있다.

재수탁측면은 기존의 수탁사-재수탁사 계약방식에서 위탁사의 동의를 확인할 수 있는 위탁사 동의 항목을 추가하여 구성한다. 해당 과정을 통해 재수탁사의 개인정보보호 역량을 확인하고, 해당 계약을 통해 재수탁사에 대한 위탁사의 관리가 이루어질 수 있도록 한다. 또한 수탁사가 점검하기 어려운 규모의 재수탁사를 위탁사를 통해 점검할 수 있는 관계를 성립할 수 있도록 한다.

계약서에는 재수탁되는 업무, 제공되는 개인정보, 개인정보보호 교육, 제3자 개인정보 유출 금지, 위반에 대한 손해배상 등이 포함되어 있어야 한다.

계약이 체결된 이후, 재수탁사는 위탁받은 업무에 대한 보호 방안 문서를 작성하고 제출하도록 한다. 재수탁사가 사전에 작성한 문서가 존재하더라도, 제공받는 개인정보가 기존에 관리하던 개인정보 항목이 아닐 수 있으므로 별도의 문서로 작성하고 이행하도록 한다.

재수탁에 대한 문서를 기준으로 개인정보보호 수행 여부 확인을 위해 정기적인 점검이 필요하다. 기존의 위탁사와 수탁사 관계에서 기업의 규모와 업무의 특성으로 인해 수행이 어려운 경우가 존재한다. Fig. 1은 그러한 관계를 보여주는 그림으로 정기적인 점검 이외에도 교육 등에 대한 부분도 동일하다. 기존의 위수탁 관계를 해석할 때에 수탁사가 재수탁사를 직접 점검하도록 되어있으나, 개인정보보호법 법령 개정에 따라 위탁사가 재수탁사를 직접 점검하여 위탁 업무가 안전하게 수행되는지 점검하는 것을 제안한다. 해당 방법은 위탁사가 재수탁사를 점검할 수 있는 역량이 있어야만 가능한 방법이기에 현실성을 고려한 자체 점검 이후 결과를 전달하는 방식 또한 제안하고자 한다. 자체점검 수행결과를 위탁사가 검토하고, 안전성 여부를 확인하는 방법으로 현실성이 결여되어 점검 자체를 진행하지 못했던 부분에 대한 해소가 가능하다. 개인정보보호 교육 또한 이와 같은 이유로 자체적인 교육을 수행하고, 이수증을 확인하는 방식으로 수행한다.

접근권한 이력 및 접속기록 이력 관리는 수탁사 점검과 마찬가지로 위탁사에서 해당 내역을 관리토록 한다. 위탁 업무를 담당하는 개인정보 취급자에 대한 보안서약서 징구 방식 또한 위-수탁 관계와 동일하게 적용한다.

개인정보 취급 단말기, 시스템 등에 대한 사전 동의 신청 방식은 개인정보 이용에 대한 이력을 명확하게 관리하고, 목적 외에 사용을 방지하는 등 불필요한 외부 노출 및 유출을 방지하기 위함이다.

4. 개인정보보호 점검항목 비교

수탁사를 위한 개인정보보호 점검항목이 부재하여 명확한 비교 대상이 부재함에 따라 개인정보보호법에 따라 개인정보를 처리하는 기업이 준수해야 하는 항목 및 위수탁사 준수사항 등을 기준을 비교하도록 한다.

개인정보보호 준수사항은 위수탁 관계가 아닌 개인정보를 취급하는 기업을 기준으로 제안되어 있음에 따라 위탁업무를 수행하는 수탁사에도 동일한 기준으로 적용하였다. 이와 더불어 개인정보처리 위수탁 관계에 대한 내용을 추가하여 정의하였다. 제안하는 수탁사 점검항목은 기존의 항목과 수행하는 주체 및 보관·관리하는 주체가 변경됨을 통해 기존보다 현실적인 접근과 개인정보의 안전한 관리가 가능토록 하였다. 위탁받은 개인정보 업무에 대한 생명주기를 수탁사가 보유한 개인정보와 분리하여 순환할 수 있도록 하였으며, 위·변조의 위험 및 악의적인 사용자에 대한 접근을 차단할 수 있도록 보관·관리 주체를 위탁사로 변경하였다. 개인정보보호법 개정에 따라 가장 큰 영향을 받는 재수탁 관련 업무는 수탁사와 재수탁사 간의 관계에서 위탁사를 포함한 관계로 재정의하고, 관리가 어려운 재수탁사에 대하여 위탁사가 영향력을 행사할 수 있도록 제안하였다.

Table 9는 제안하는 점검항목이 이행가능 여부에 대한 평가를 수행한 결과다. 기업의 규모 여부에 관계없이 적용 가능성을 평가한 것으로, 점검을 유지하기 어려운 영세기업을 중점으로 평가하였다. 물리적인 보안방안에서 별도의 사무실 구비가 어려운 기업은 업무영역을 분리하고, 개인정보에 대한 접근을 통제함으로서 기존에 준수하기 어려운 물리적 방안을 준수할 수 있도록 하였다. 기술적인 부분에서 접근권한 및 접속기록 관리가 어려울 가능성이 있는 부분은 위탁사에서 관리하도록 함으로서 수탁사가 감당해야할 부담감을 해소하였다. 가장 큰 변화와 효과를 도출한 재수탁은 영세기업보다 규모가 큰 재수탁사에 대한 보안점검을 진행할 수 있는 가능성을 제시함으로서 다양한 환경에서도 재수탁 관리가 용이할 수 있도록 하였다.

Table 8. Compare of Proposal Check List

	Personal information protection compliance list	Suggested consignee inspection list
Management	Privacy Policy Document for Corp	Privacy policy document for consignment work
	Appointment of personal information protection officer	Appointment of personal information manager for entrusted work
Physical	Office access control	Separation of work areas (control access of outsiders if necessary)
	Access control to restricted areas	Personal information access control
Technical	Personal information security measures	
	(Trustee)Personal information protection and management	(Consignor)Personal information protection and management
	(Trustee)Personal information protection status management	(Consignor)Personal information protection status management
Life-Cycle	Check of protection measures according to personal information life cycle	
Re-entrustment	Consignor-sub-consignee contract structure	Consignor - Structure of the original consignor's consent to the sub-consignor contract
	Apply to existing internal management plans and regulations, etc.	Separate security management document for consignment-related contents
	Direct inspection by the consignee of the re-consignee	Self-Check by the re-consignor or inspection by the original consignee
	The subtrustee independently manages access rights and usage history.	Management of access rights and use history of original consignee
	Security pledge for re-trustees	Request for security pledge from the representative(CEO)
	Conducting personal information protection training for sub-trustees	The subtrustee conducts personal information protection training on its own.
	-	Application for prior consent for personal information access device and system

Table 9. Possibility of Compliance Compared to Existing

Domain		Personal information protection compliance list	Suggested consignee inspection list
Management	Privacy Policy Document	O	O
	Appointment of personal information protection officer	O	O
	Personal information access device and system	X	O
Physical	Office access control	△	O
	Access control to restricted areas	△	O
Technical	Personal information protection and management	△	O
	Personal information protection status management	△	O
Life-Cycle	Personal information life cycle	O	O
Re-entrustment	Consignor-sub-consignee contract structure	O	O
	security management document	△	O
	Check by the re-consignor	△	△
	Management of access rights and use history	△	O
	Security pledge for re-trustees	△	O
	Protection training	△	O
	Personal information access device and system	X	O

이를 통해 현실적으로 수행이 어려웠던 부분에 대한 해소가 가능할 것으로 예상되며, 수탁사의 개인정보보호 부담을 완화시키는 효과가 있다. 이는 특히 재수탁사보다 규모가 영세한 수탁사에게 효과적으로 적용할 수 있을 것으로 보인다.

5. 결 론

본 논문에서는 개인정보 업무 위탁사 관리에 대한 간단한 프레임워크와 개인정보보호 점검을 위한 필수 공통의 점검항목을 제안하였다. 개인정보 업무 위탁사 관리 프레임워크는 계약-이행-종료의 3단계 구성을 통해 각 단계별로 요구되는 필수적인 내용을 정의함으로써 기존의 위수탁 계약에 보다 효과적인 보안관리가 가능하도록 하였다. 기존의 위수탁 계약 방식과 유사하지만, 개정된 개인정보보호법의 재수탁 관련 내용을 반영하여 법적 준거성을 확보하도록 하였다.

개인정보보호 점검항목은 관리적, 물리적, 기술적, 생명주기, 재수탁의 5가지 측면으로 업무영역 및 특성에 상관없이 필수 공통사항을 제안하였다. 특히 재수탁 관련 항목에 현실성을 고려함으로써 영세한 수탁사의 부담을 완화할 수 있도록 하였다. 수탁사의 부담 완화를 통해 더욱 필요한 부분에 보안을 강화할 수 있도록 하고, 상대적으로 규모 차이가 심함 재수탁 관계에서도 개인정보의 안전한 관리가 이루어졌으면 하는 바람이다. 제안하는 점검항목을 통해 개인정보 업무 위탁 과정에서 발생할 수 있는 위험성을 최소화하여 개인정보 유출 등의 사건·사고를 사전에 예방하는데 기여할 수 있었으면 한다.

References

[1] S. J. Jeon, "Outsourcing, provision or joint controlling the personal information," *Journal of Korea Infomation Law*, Vol.26, No.3, pp.193-235, 2022.

[2] D. H. Park, "Trendsof information security and privacy international standardization," *Review of KIISC*, Vol.23, No.4, pp.47-52, 2013.

[3] D. S. Im, "An empirical study between checking activity of management level of consignee's personal information protection and information security performance," *Journal of Information Technology and Architecture*, Vol.15, No.1, pp.31-42, 2018.

[4] Korea Internet & Security Agency [Internet], https://www.kisa.or.kr, Information Protection and Certification Standards Guide Personal Information Protection Management System (ISMS-P) Certification Standards Guide.

[5] Y. D. Ko, "A proposal of enhanced personal information security management framework of consigning of personal information," *Journal of The Korea Institute of Information Security & Cryptology*, Vol.25, No.2, pp.383-393, 2015.

[6] S. T. Hyun, "A study on the enforced security of personal information outsourcing," *Journal of Korea Safety Management & Science*, Vol.16, No.3, pp.433-441, 2014.

[7] Ministry of Government Legislation [Internet], https://www.law.go.kr, Personal Information Protection Act.

[8] Personal Information Protection Commission [Internet], https://www.pipc.go.kr, Personal information processing entrustment guide.

박 유 림

https://orcid.org/0009-0007-0662-979X
e-mail : yrbak08@naver.com
2017년 숭실대학교 컴퓨터공학과(석사)
2022년 숭실대학교 컴퓨터공학과(박사수료)
2022년 ~ 현 재 한국국방연구원
국방데이터분석센터 연구원
관심분야 : Information Security, Privacy, Data Architecture

신 용 태

https://orcid.org/0000-0002-1199-1845
e-mail : shin@ssu.ac.kr
1985년 한양대학교 산업공학과(학사)
1990년 Univ. of Iowa, 컴퓨터공학과(석사)
1994년 Univ. of Iowa, 컴퓨터공학과(박사)
1995년 ~ 현 재 숭실대학교 컴퓨터학부 교수
관심분야 : 정보보호, 인터넷 프로토콜, IoT, 클라우드 컴퓨팅