J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

군장병 휴대전화 사용제도 시행에 따른 개인정보 안정성 확보 방안 연구☆

A Study on ways to secure personal information stability according to the implementation of the mobile phone use system for militaryary personnel

황 보 원 규[1] 신 동 규[1,2,3*]
Wongyu Hwangbo Dong-Kyoo Shin

요 약

군장병의 일과 후 병 휴대전화 사용을 전면 허용함에 따라 휴대전화 개통시 통신사에서 개인정보 직접 수집을 최소화 하여 군장병의 개인정보 안정성 확보가 필요한 시점이다. 국방부는 일과 후 군장병의 휴대전화 사용을 도입하기에 앞서 사이버 불법도박, 게임중독, 음란물 시청 등 일부 역기능에 대한 우려 및 보안사고 예방을 위해 휴대전화 촬영기능을 차단하는 등의 보안통제 체계를 구축해 왔다. 이동통신사는 통신대리점에 휴대전화 개통 등 개인정보 처리업무를 위탁하고 개인정보 보호조치 실태점검 등 관리감독을 수행하지만 통신대리점에서 위탁업무 목적외로 개인정보의 수집하는 행위가 발견되고 있다. 군장병이 휴대전화를 개통할 경우 개인정보 이동권을 활용하여 개인정보관리 전문기관을 신설하고 개인정보관리 전문기관에 군장병의 개인정보 전송을 요구하는 체계를 제시한다.

☞ 주제어 : 군장병 휴대전화, 개인정보보호, 통신대리점, 안전한 활용, 마이데이터, 개인정보 이동권

ABSTRACT

As military service members are fully permitted to use mobile phones for sickness after work, it is time to minimize the direct collection of personal information from telecommunication companies when opening mobile phones to secure the safety of military service personnel's personal information. Prior to introducing the use of mobile phones by soldiers after work, the Ministry of National Defense established a security control system such as blocking the mobile phone shooting function to prevent security accidents and concerns about some adverse functions such as illegal cyber gambling, game addiction, and viewing pornography. come. Mobile telecommunications companies entrust personal information processing tasks, such as opening mobile phones, to telecommunications agencies and carry out management and supervision, such as checking the status of personal information protection measures. When a military service member opens a mobile phone, a personal information management agency is newly established using the right to portability of personal information, and a system for requesting the transmission of personal information from the military service member is proposed.

☞ keyword : Military mobile phone, personal information protection, telecommunication agency, safe use, my data, right to transfer and port personal information

1. 서 론

국방부는 '국방개혁 2.0' 추진과 함께 '일과 후 병 휴대전화 사용'이 민·군 융합을 통한 개방형 국방운영과 인권존중의 선진병영문화 정착 등에 기여할 것으로 판단하여 의무복무 병사를 독립된 인격체로 대우하고 군 복무로 인한 고립감 해소, 자기개발, 건전한 여가 선용 등을 위해 일과 이후(휴일 포함)에 한하여 휴대전화 사용 정책을 도입하였다. 국방부 직할 4개 부대를 대상으로 2018년 4월부터 일과 후(18:00 ~ 21:00), 휴무일(08:30 ~

1 Department of Computer Engineering, Sejong University, Seoul, 05006, Korea.
2 Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul, 05006, Korea.
3 Department of Cyber Warfare Research Center, Sejong University, Seoul, 05006, Korea.
* Corresponding author (shindk@sejong.ac.kr)
[Received 30 August 2022, Reviewed 17 September 2022(R2 23 October 2022), Accepted 7 November 2022]
☆ 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1F1A1074773).

21:00)에 휴대전화 사용 시범운영을 시작하였다. 2019년 4월에는 GP, 훈련병을 제외한 전 부대를 대상으로 시범운영 후 각종 규정과 제도를 정비하고, 보안통제 체계(국방 모바일보안 앱)를 개발 구축하였다. 27개월간의 시범운영을 분석한 결과 다양한 긍정적인 측면이 확인되어 군인복무정책 심의위원회(2020.6.26.)를 거쳐 2020년 7월 1일부로 전면 시행하였다. 또한, 건전한 휴대전화 사용 문화를 정착시키고 역기능을 최소화하기 위하여 자율과 책임하에 휴대전화를 사용·관리하고 휴대전화로 인한 사건·사고 발생 시 적절한 책임을 부과하게 하였다 [1].

이동통신사는 통신대리점과 위탁계약 체결을 통해 상품 및 서비스 가입 등에 관한 업무와 그 부대업무의 대행, 요금수납에 관한 업무 및 그 부대업무 등을 포함하여 고객관리 업무의 대행, 고객에 대한 사후 서비스 업무의 대행 업무를 위탁하고 있다.

통신대리점은 군장병의 휴대전화 개통 요청이 발생하면 관련 부대업무 대행을 위하여 이동통신사의 고객관리 시스템을 통해 이용자의 개인정보를 저장 및 조회하며 업무 처리를 할 수 있다. 통신대리점은 위탁업무를 수행하는 과정에서 취득한 군장병의 개인정보를 위법하거나 부당하게 유출 또는 사용하거나, 제3자로 하여금 위법하거나 부당하게 유출 또는 사용하게 함으로써 이득을 취할 수도 있다. 이동통신사는 이러한 경우를 예방하기 위하여 개인정보 보호조치 준수 및 위반시 계약해지와 손해배상의 의무를 부여하도록 계약서에 명시하고 있다.

매년 이동통신사는 통신대리점에 대한 개인정보 보호조치 관리·감독의 의무를 다하기 위하여 개인정보 처리시 보호조치 의무 이행 여부에 대한 실태점검을 시행하고 발견된 미흡사항은 개선조치 요구 등의 노력을 지속하고 있지만 반복되는 미흡사항에 대해 실효성있는 통제에는 어려움을 겪고 있다.

최근 개인정보의 안전한 활용을 위해 데이터3법(개인정보보호법, 정보통신망법, 신용정보법)의 개정이 이뤄졌고, 신성장 동력이 되는 4차 산업 혁명은 데이터를 기반으로 이뤄지고 있다. 대부분의 서비스 산업은 개인정보를 기반으로 모델링이 이뤄지고 각종 맞춤형, 이용자의 동선을 기반으로 한 상권분석 등 개인데이터로부터 시작되고 있기 때문에 프라이버시의 보호는 최우선 과제가 되고 있다 [2].

국방부는 일과후 군장병의 휴대전화 사용 도입에 앞서 사이버 불법도박, 게임중독, 음란물 시청 등 일부 역기능에 대한 우려 및 보안사고 예방을 위해 휴대전화 촬영기능을 차단하는 등의 보안통제 체계를 구축하여 왔다 [3]. 그러나, 통신대리점에서 개통처리를 하는 과정에서 군장병의 개인정보를 개통 등의 업무위탁 목적이외로 수집하는 경우의 개인정보 안전성 확보조치에 대해 충분한 검토가 이뤄지지 않았다.

본 연구는 군장병이 휴대전화 사용을 위해 개통 할 경우 개인정보 이동권을 활용하여 통신분야 개인정보관리 전문기관을 통해 군장병의 개인정보를 저장·관리하고 이동통신사 간 데이터 이전을 중개하는 플랫폼을 구축하여 통신대리점에서는 군장병의 개인정보를 직접 수집하지 않고 통신서비스 상품을 판매할 수 있도록 안전한 환경을 구축 할 수 있는 방안을 제시한다.

2. 관련 연구

2.1 개인정보의 안전성 확보

2.1.1 휴대전화 사용에 따른 국방부의 군장병 개인정보 이용

국방부는 군장병의 성명, 휴대전화번호, 군번, 입대일 및 전역일 등의 개인정보를 수집하고 보직, 진급, 징계, 전역 등 군장병 복무관리를 위하여 이용하고 있다.

국방부는 군장병의 헌법상 기본권을 보장하기 위하여, 일과후 휴대전화 사용을 전면 허용하면서 군장병이 휴대전화를 이용한 불법도박 사례가 증가하고 있기 때문에 불법도박 이용 예방 및 건전한 병영생활을 위하여 군장병의 휴대전화에 불법도박 예방 프로그램을 의무설치·운용하는 정책을 추진하고 있다.

국방부는 기존에 수집하여 보유중인 군장병의 개인정보를 개인정보보호법 제15조 제1항 제3호에서 개인정보처리자는 '공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우'에 개인정보를 수집·이용할 수 있다는 규정에 따라 다음의 소관업무를 적용하고 있다 [4].

1) 국방부와 그 소속기관의 직제 제13조 제3항 제8호에서 군인의 복제·'군기'·안전·상훈·군예식 및 행사에 관한 사항을 국방부의 분장사무로 정하고 있다.
2) 군인복무기본법 시행령 제2조 제1호에 따르면 '군기'는 지휘체계 확립, 질서 유지, 전투력 보존·발휘 등을 위하여 법규와 명령을 준수하고 일정한 방침에 복종하는 것을 의미한다.
3) 국방 사이버기강 통합관리 훈령 제4조 제1항, 제2항 및 제4항은 '사이버기강 저해 사이트 여부 검토, 사이버기강 저해사이트 접속 차단 체계 관리 및 사이버기

강 저해 사이트 접속 차단 전파' 등을 국방부의 업무로 규정하고 있다 [4].

2.1.2 EU, GDPR

GDPR*은 자연인(natural person)에 관한 기본권과 자유 및 특히 개인정보보호에 대한 권리를 보호하고, EU 역내에서 개인정보의 자유로운 이동을 보장하는 것을 목적으로 하며, EU 밖에서 EU 내에 있는 정보주체에게 재화나 용역을 제공하는 경우, 또는 EU 내에 있는 정보주체가 수행하는 활동을 모니터링하는 경우에 적용한다 [5]. 개인정보를 처리하는 경우 다음 7가지 원칙을 모두 준수하여야 한다.

1) 합법성·공정성·투명성 원칙
2) 목적 제한의 원칙
3) 개인정보 최소처리 원칙
4) 정확성의 원칙
5) 보유기간 제한의 원칙
6) 무결성과 기밀성의 원칙
7) 책임성의 원칙

또한, 수집되는 개인정보가 이용되는 목적에 대한 명시적 동의여야 하며, 다음 중 어느 하나 이상의 요건에 해당해야 합법 처리로 인정된다.

1) 정보주체가 하나 이상의 특정한 목적을 위하여 본인의 개인정보 처리에 동의한 경우
2) 정보주체가 계약당사자로 있는 계약의 이행을 위하여 또는 계약체결전 정보주체의 요청에 따라 조치를 취하기 위하여 처리가 필요한 경우
3) 컨트롤러**에 적용되는 법적 의무를 준수하는 데 처리가 필요한 경우
4) 정보주체 또는 자연인인 제3자의 생명상의 이익을 보호하기 위하여 처리가 필요한 경우
5) 공익상의 이유 또는 컨트롤러에게 부여된 직무권한을 행사할 때 처리가 필요한 경우
6) 컨트롤러 또는 제3자의 적법한 이익을 달성하기 위하여 처리가 필요한 경우

2.1.3 EU, 개인정보 이동권

유럽연합은 개인정보 이동권을 도입하여 온라인 서비스에 대한 정보주체의 선택권을 확대하고 데이터에 대한 독점을 완화하여 기업 간 공정한 경쟁 환경을 조성하였다. GDPR 제20조 ' (Right to data portability)'는 정보주체가 컨트롤러에게 제공한 본인의 개인정보를 체계적으로 구성하여, 기계 판독이 가능한 형식으로 제공받을 권리를 의미한다. 정보주체는 기술적으로 실현 가능한 경우 개인정보가 한 정보 관리자에게서 다른 정보 관리자에게로 직접 전송되도록 할 권리가 있다.

모든 정보가 개인정보 이동권의 대상은 아니며, 정보주체가 컨트롤러에게 제공한 개인정보로서 처리가 정보주체의 동의에 근거하거나 계약의 이행을 위한 것이며 처리가 자동화된 수단에 의해 이루어지는 개인정보인 경우 정보의 산출 요건만 만족하면 행사가 가능하다 [5].

2.1.4 국내, 개인정보 보호법

개인정보 보호법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.

개인정보를 처리하는 경우 다음의 주요 원칙을 모두 준수하여야 한다.

1) 개인정보처리자***는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
2) 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
3) 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
4) 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다 [6].

* 2016년 5월 유럽연합(이하 'EU')에서 제정한 '일반 개인정보 보호법(General Data Protection Regulation)' (이하 'GDPR')이 2018년 5월 25일부터 시행되었다.

** 개인정보 처리의 목적과 수단을 결정하는 주체를 의미하며, 이와 같은 결정은 컨트롤러 단독으로 하거나 또는 제3자와 공동으로 할 수 있다. 자연인을 비롯하여 법인, 정부부처 및 관련기관, 기타 단체 등이 컨트롤러가 될 수 있다.

*** 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

2.1.5 국내, 마이데이터 산업 추진 현황

정부는 2016년 “지능정보사회 중장기 종합대책”에서 K-MyData를 발표하였고, 4차산업혁명위원회는 ”데이터 산업 활성화 전략“을 2018년에 발표하였다 [7]. 금융 분야는 2018년부터 금융분야 마이데이터 산업 도입 계획에 대하여 발표하였고 2019년에는 개인신용정보의 안전한 전달체계 마련을 위해 데이터 표준 API (Application Programming Interface, 응용 프로그램 인터페이스) 구축 계획을 발표하였다. 2020년에는 신용정보법 개정 시 금융분야의 마이데이터 산업추진의 법적 근거를 마련하였다. 행정안전부는 정부가 보유하고 있는 개인의 행정 정보에 대하여 정보주체의 검색・저장・유통이 가능하도록 마이데이터 시스템을 구축하여 각종 행정처리 업무 신청에 구비서류 대신 꼭 필요한 데이터만 제공하여 자격증명을 할 수 있도록 공공부문 마이데이터 사업을 추진 중이다 [8]. 본인이 요청 할 경우 공공부문이 보유한 개인정보를 제3의 기관에 전송할 수 있도록 공공부문에 대한 개인정보 전송권 도입을 검토 중이다 [9].

2.2 이동통신사의 개인정보 보호조치 현황

2.2.1 이동통신사의 개인정보보호조치 관리・감독

이동통신사는 통신대리점에게 제공한 정보 및 제공된 정보를 통신대리점 및 통신대리점의 사용인・종업원 등은 가공, 복제, 조합하는 방법을 포함하여 모든 정보를 타인에게 누설하거나 직접 또는 제3자가 이용하게 하여서는 아니되며 ‘영업비밀 및 개인정보’의 보호의무를 부여하고 이러한 의무 이행에 대한 관리・감독의 책임을 정하고 있다. 이동통신사는 통신대리점에게 고객정보 관리・감독에 관한 보호의무를 준수 하도록 요구하고 보호의무를 위반할 경우 통신대리점은 관련 법령 및 위탁계약에 따른 책임을 분담하고 손해배상을 하여야 한다.

2.2.2 개인정보 위・수탁시 관리・감독 사항

이동통신사는 통신대리점과 상품 및 서비스 가입 등에 관한 업무에 대해 위탁계약을 체결하고 있으며, 통신대리점은 이동통신사의 사전 서면 동의 없이 계약상 위탁된 업무를 제3자에게 재위탁할 수 없으며, 통신대리점이 영업활성화를 위하여 제3자에게 위탁받은 업무를 일부 대행하게 하는 재위탁점 또는 분점을 두고자 하는 경우에도 재위탁점 및 분점의 상호, 소재지 등 제반자료를 통신사에 사전 신고하고 합의하여야 한다. 대행업무의 범위는 통신사와 합의하여 정하여야 한다. 재위탁점은 고객에 대한 관리업무 및 고객에 대한 사후 서비스 업무를 대행할 수 없다.

재위탁점은 통신사의 상품 및 서비스 가입에 관련한 범위에 대해서만 수행하여야 하며 고객에 대한 관리업무 및 고객에 대한 사후 서비스 업무를 대행하기 위한 개인정보를 보유할 수 없다. 또한, 통신대리점은 분점 또는 재위탁점의 행위로 인하여 발생 된 통신사 및 고객의 손해에 대하여 책임을 부담하여야 한다.

2.3 통신대리점의 개인정보 보호조치 위반 현황

2.3.1 개인정보 보호조치 위반 신고 사례

개인정보 보호 상담사례집(한국인터넷진흥원, 2019년)에 따르면 개인정보 침해 신고 사례의 주요 내용은 보이스 및 메신저 피싱 등 전자 통신 금융사기 관련 상담이 큰 폭으로 증가, 개인정보 미파기 신고 상담 증가, 적법하지 않은 주민등록번호 처리 관행이다. 특히, 개인정보 침해 신고의 경우 개인정보의 수집, 이용, 제공, 보유 목적을 달성한 경우 복구, 재생할 수 없는 방법으로 파기하여야 함에도 불구하고 사업자가 해당 개인정보를 파기하지 않고 보유하거나 파기하여야 할 개인정보 서류를 무단 투기하는 경우로써 2019년 1,214건의 신고가 접수되었다 [6].

이동통신사는 개인정보 처리 업무를 위탁받은 통신대리점에 대한 개인정보 위・수탁 및 관리・감독 현황을 살펴보면 업무위탁 범위를 영업 및 고객 유치에 한정하고 개통업무가 완료 된 이용자의 개인정보는 현장에서 즉시 파기하도록 하여 통신대리점이 자체적인 목적으로 개인정보를 별도로 보관하는 행위를 금지하고 있다. 통신대리점의 수행업무를 살펴보면 고객 민원 대응도 처리하고 있기 때문에 민원 대응 및 해소를 목적으로 개인정보를 보관하는 경우도 발생하기 때문에 통신대리점에서의 개인정보 유출 사고 발생 위험이 높아지고 있다.

3. 개인정보의 안전성 확보조치 위반 사례

3.1 개인정보 안전성 확보조치 위반시 제재

3.1.1 개인정보보호법 관련 위반시 처벌

개인정보보호위원회고시에서 정한 개인정보보호 법규 위반에 따른 과징금 부과에 필요한 세부기준을 살펴보면 위반행위의 중대성의 판단 기준 중 고의・중과실 여부는 영리 목적의 유무, 안전성 확보조치 이행 여부 등을 고려

하여 판단한다. 관련하여 개인정보보호법에 따른 안전성 확보조치 위반시 처벌 사항은 표 1과 같다.

(표 1) 개인정보보호법 관련 위반 유형별 처벌 사항
(Table 1) Punishment by type of violation related to the Personal Information Protection Act

위반사항	근거	처벌규정
주민등록번호 (신분증)보관	제24조의2 (주민등록번호 처리의 제한)	- (유출시)5억원 이하의 과징금 - 5천만원 이하의 과태료
개인정보의 파기	제21조(개인정보의 파기)제1,2항	- 2년이하의 징역 또는 2천만원 이하의 벌금 - 3천만원 이하의 과태료
개인정보의 안전조치 의무	제29조(안전조치 의무)	- (유출시)2년이하의 징역 또는 2천만원 이하의 벌금 - 3천만원 이하의 과태료

3.1.2 개인정보 안전성 확보조치 위반 사례

통신대리점에서 업무수탁 범위를 벗어나 통신대리점 자체적인 영업 및 고객 유치에 활용하기 위한 목적으로 개인정보를 별도 보관하는 대표적인 사례는 표 2와 같다.

(표 1) 개인정보 불법 수집 사례
(Table 1) Cases of illegal collection of personal information

No.	내용
1	위탁업무 목적외로 개인정보파일을 수집
2	이용목적 달성 또는 보관기관이 경과한 개인정보의 미파기
3	개인정보의 과다수집
4	신분증 사본/스캔본의 별도 보관

3.1.2 개인정보 안전성 확보조치 위반사례 별 위험도 분석

개인정보보호위원회 등의 규제기관은 개인정보 보호법령 위반 수준에 따라 과태료 및 과징금 처분 수위를 결정하고 있으며, 사안에 따라, 수사기관 이첩, 위반 내용 및 처분결과 대외 공표 등을 병행하며, 처분 정도를 결정하는 주요 기준은 개인정보 미파기 수량 및 기간 등이 있다. 따라서, 규제기관의 과태료 및 과징금 처분 사례를 기반으로 본 연구에서 개인정보 안전성 확보조치를 위반한 사례별로 위험도를 분류하였다.

1) 미파기 수량

(구)방통위는 개인정보 미파기 건수가 1천건 이상인 경우 수사기관(검찰)에 이첩하도록 규칙을 적용하였다.

개인정보위는 수사기관 이첩에 대한 규칙을 따로 규정하진 않았으나 행정처분의 연속성 등을 감안할 때 1천건 이상인 경우 수사기관에 이첩할 가능성이 매우 높다.

최근 통신사(위탁자) 행정처분(2020.12.9.) 사례를 보면 개인정보 미파기 적발 수준이 1만 4천여 건으로, 1만건 이상 적발 시 위탁자에도 추가 조사가 이뤄질 가능성이 매우 높다.

(표 3) 미파기 수량 위험도
(Table 3) Undestroyed Quantity Risk

미파기 수량	1만건 이상	1만건 미만, 1천건 이상	1천건 미만
위험도 등급	심각	경계	주의

2) 법규 위반 기간

이동통신사 및 통신대리점에 대한 행정처분(2020. 12. 9.) 사례를 보면 개인정보 미파기 기간이 1년 이상 경과된 개인정보가 다수 적발되었고 이에 따라 이동통신사는 수탁자에 대한 관리·감독이 정상적으로 이뤄진 것으로 볼 수 없다고 판단하였다.

개인정보보호위원회는 통신대리점과의 위·수탁계약이 매년 갱신되고 있으므로 이에 따라 관리·감독이 최소 1년에 한번은 해야 한다고 판단하고 있다.

법 위반 기간이 3개월 이상인 경우 과태료 기준 금액 50% 가중처분 사유에 해당되며, 개인정보보호법 제66조에 따라 조사 결과 및 처분 내용이 개인정보보호위원회 홈페이지에 공표되어 이동통신사의 이미지에 심각한 훼손이 발생할 수 있다.

(표 4) 법규 위반 기간 위험도
(Table 4) Violation period Risk level

미파기 기간	1년 이상	1년 미만, 3개월 이상	3개월 미만
위험도 등급	심각	경계	주의

3) 고객관리번호 별도 보관 행위

이동통신사에 대한 행정처분(2020. 12. 9.) 사례를 보면 이동통신사 영업전산시스템에서만 사용되어야 하는 고객관리번호가 통신대리점 영업시스템에 저장·관리되

고 있는 점을 들어 개인정보 유출로 간주하였다.

고객관리번호는 이동통신사 영업전산시스템에 업무 목적별로 분산 저장되어 있는 고객의 모든 정보를 연동하거나 각종 조회 및 수정 시에 사용되는 키값과 같은 정보이다.

(표 5) 고객관리번호 별도 보관 위험도
(Table 5) Risk level of separate storage of customer management number

보관 정보	고객관리번호	주민등록번호	그 외 개인정보
위험도 등급	심각	경계	주의

4. 개인정보의 안전성 확보조치 실태점검

4.1 개인정보보호 실태점검 수행

본 연구에서는 통신대리점이 자체적인 영업활동 및 고객 유치에 활용하기 위해 이동통신사의 업무 위탁 목적 외로 개인정보를 음성적으로 처리하는 행위 등의 안전성 확보조치 위반 사례에 대해서 실태점검를 수행하였다.

4.1.1 실태점검 절차

실태점검은 전국에 분포해 있는 이동통신사의 통신대리점 1,000개소를 대상으로 2021년 7월부터 10월까지 4개월에 걸쳐 시행하였으며, 개인정보 관련 표 6과 같은 주요 행정처분 사례를 반영하여 표 8의 점검항목을 기반으로 현장 실사를 통해 이루어 졌다. 실태점검의 독립성 및 객관성을 보장하기 위하여 개인정보보호협회를 통해 규제기관 조사지원 또는 이동통신사 대리점 개인정보보호 현장 실태점검 유경험자로 구성된 점검반을 통해 이루어졌다.

(표 6) 개인정보 관련 행정 처분 사례
(Table 6) Administrative disposition cases related to personal information

이상징후	설명
업무목적 달성 시 미파기	개통, 정산처리 등 수집된 개인정보의 이용목적이 종료된 경우 즉시 파기를 하지 않은 경우
보관기간 경과 시 미파기	서비스 해지후 6개월이 경과한 즉시 파기하지 않은 경우
보호조치 미준수	개인정보 저장 및 전송시 암호화 조치 등 안전한 처리를 하지 않은 경우
주민등록번호 수집 위반	관련 법에서 정하지 않은 이유로 수집이 이루어진 경우

4.1.2 실태점검 결과

위탁대리점에서 개인정보 처리업무 수탁 범위를 벗어나 대리점 자체적인 영업 및 고객 유치에 활용하기 위한 목적으로 개인정보를 위법하게 음성적 보관행위를 한 경우 위험도 분석 기준을 바탕으로 실태점검 결과를 재구성 하면 표 7과 같다.

(표 7) 이상행위 사례별 위험도 분포
(Table 7) Risk distribution by abnormality case

항목	주의	경계	심각
업무목적 달성 시 미파기 수량	70.3%	23.8%	5.9%
보관기간 경과 시 미파기 기간	34.9%	29.1%	36.0%
보호조치 미준수 기간	33.2%	29.7%	37.1%
주민등록번호 수집 위반	55.7%	24.9%	19.4%

실태점검은 통신대리점 내 문서보관함, 사물함, 선반, 창고 등 물리적인 상면과 대리점 내 전산장비(PC, 노트북, 태블릿, USB 등)를 대상으로 점검반이 현장에 직접 방문하여 체크리스트 기반으로 개인정보보호법 및 이동통신사 정책 위반여부를 확인하는 방법으로 수행한 세부 점검결과는 표 8과 같다.

(표 8) 실태점검 시 발견된 안전조치 위반 현황
(Table 8) Status of violations of protection measures found during fact-finding inspection

분류		점검결과(건수)			합계 (건수)
		A	B	C	
개인정보 파기	파일	230	227	84	541
	서류	211	179	114	504
	비인가서식	138	29	41	208
주민등록번호	신분증	202	173	87	462
	복사본	78	9	36	123
	위변조	3	2	2	7
기술적 보호조치	암호화	191	202	59	452
	잠금장치	181	167	100	448
	계정공유	117	21	19	157
	퇴사자관리	55	17	10	82
PC 보호조치	비밀번호	94	193	90	377
	화면보호기	103	239	79	421
	업데이트	52	77	48	177
	실시간감시	7	7	13	27
보안시스템 설치	백신	8	2	7	17
	개인정보탐지	96	26	38	160
	DRM	9	0	5	14
	DLP	3	1	4	8
합계		1778	1571	836	4,185

5. 휴대전화 개통시 군장병 개인정보의 안전성 확보조치 방안

5.1 휴대전화 개통시 개인정보 보호조치 한계

5.1.1 휴대전화 개통시 개인정보 직접 수집 한계

이동통신사는 개인정보 처리를 업무위탁 한 통신대리점에 대해 개통업무가 완료 된 고객 개인정보는 현장 즉시 파기하고 통신대리점 자체적으로 별도로 개인정보 보관행위를 하지못하도록 금지하고 있지만 개인정보를 파기하지 않고 보유하거나 파기하여야 할 개인정보 서류를 무단으로 보관하는 행위가 지속되는 것을 확인할 수 있었다.

이통동신사는 지속적인 점검활동 및 교육 등 관리적 보호조치 수행, 지류서식지를 온라인 신청서로 대체하도록 기술적 보호조치 등을 수행하고 있음에도 불구하고 개인명의로 발급되는 휴대전화 개통을 위해서는 군장병의 개인정보를 기반으로 할 수밖에 없는 상황이다.

5.1.2 이동통신사의 재위탁점 관리·감독 한계

이동통신사는 통신대리점과 상품 및 서비스 가입 등에 관한 업무에 대해 위탁계약을 체결하고 있으며, 통신대리점은 위탁된 업무를 제3자에게 재위탁할 수 있다. 재위탁을 받은 재위탁점의 경우 국내 모든 이동통신사의 서비스를 취급하고 있는 시장구조에서는 특정 한 개의 이동통신사가 단독으로 관리·감독을 시행할 경우 재위탁점으로부터 영업방행 등의 이유로 공정위 제소, 해당 통신사에 대한 영업중단으로 유통망 축소 등 위험을 감수하여야 한다. 재위탁점들은 개인정보보호 안전조치 위반에 대한 제재가 가해지더라도 제재를 가한 이동통신사가 아닌 타통신사의 서비스도 같이 취급하므로 계속 영업이 가능하여 특정 이동통신사 단독으로 관리·감독을 수행하는 것이 개인정보 안정성 확보조치에 대한 효과성을 높이지 못하는 현실이다.

5.1.3 대리점의 재위탁점 관리·감독 한계

재위탁점은 지속적인 영업활동을 하기 위해서 통신대리점으로부터 위탁받은 개인정보 처리업무 수행 과정에서 획득한 개인정보를 위탁업무 목적외로 보관하고 있음에도 불구하고 일부 대형 통신대리점을 제외하고는 대부분을 차지하는 중소규모 통신대리점은 자체적으로 정기적인 관리·감독을 위한 인력, 예산, 전문성을 확보하기가 어렵다. 이동통신사와 동일하게 재위탁점은 다수의 타통신사에 속한 통신대리점과 재위탁계약을 맺는 영업구조를 갖추고 있기 때문에 특정 통신대리점이 단독으로 관리·감독을 하기 어렵고, 단독으로 관리를 하더라도 영업망 축소 등의 위험을 감수해야 한다.

5.2 군장병 개인정보의 안전한 활용 방안 제시

5.2.1 개인정보의 안전한 활용 사례

통신사들은 PASS앱*을 통해 운전면허증과 같이 전자신분증을 활용하기 위한 방안을 마련하고 제도적으로 국가지정 공식 신분증으로의 역할을 해나가고 있으며, 국내선 항공 탑승 시 DID** 모바일 신분증 도입도 이뤄지고 있는 상황이다.

금융권에서는 개인정보 이동권(전송권)을 활용한 마이데이터 사업을 통해 개인의 금융자산을 하나의 은행에서 관리할 수 있도록 금융분야 개인정보관리 전문기관을 운영하고 있는 실정이다 [8].

유럽연합의 경우 개인정보 자기관리시스템(PIMS: : Personal Information Management System) 또는 개인정보저장소(PDS: Personal Data Store) 도입·활용이 진행 중이고 이들은 개인이 자신의 데이터를 저장·관리하고 기업 간 데이터 이전을 중개하는 플랫폼 기능을 한다 [9].

5.2.2 휴대전화 개통시 개인정보 수집 대체 방안

이동통신 서비스의 가입신청 또는 회선추가, 타통신사로의 번호이동 등이 발생할 때마다 이용자는 가입신청서를 신규로 작성하며 매번 본인의 개인정보를 통신유통점을 통해 이동통신사에게 제공하고 있으며, 이동통신사에서도 서비스 이용자 본인확인을 하기 위한 목적으로 수집된 개인정보를 이용하고 있다.

군장병이 휴대전화 이용신청을 위해서 매번 가입신청서를 작성해야 하지만 개인정보 수집 행위가 발생하는 것이 아니라 기존에 이용 중인 서비스에 대해 본인확인 절차만 거치게 되면 이미 보유하고 있는 군장병의 개인

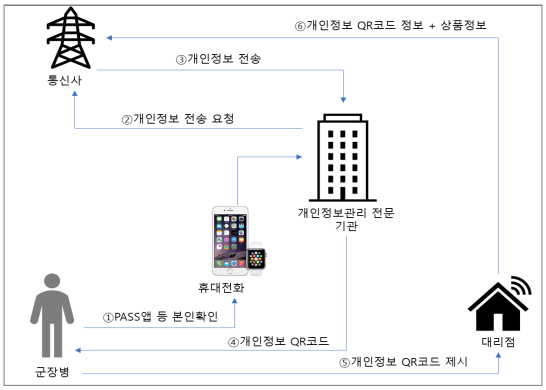
* 공인인증서 제도 폐지에 따라 SK텔레콤, KT, LGU+에서 각종 본인확인·온라인 서류발급 신청·금융거래·계약서 전자서명에 이용할 수 있도록 운영중인 앱이다.

** DID 기술은 블록체인 기술을 기반으로 개인정보를 분산하여 보관하는 기술을 활용하여 본인의 신원증명을 중앙에 의존하지 않는 탈중앙화된(decentralized) 디지털 신원증명 체계이다.

정보를 이동통신사 간 데이터 이전을 중개하는 플랫폼을 통해 서비스 개통이 된다면 통신대리점에서 직접적인 개인정보 수집 행위 자체를 제한할 수 있을 것이다.

5.2.3 통신분야 개인정보 관리 전문기관 운영

본 연구에서는 휴대전화 개통 시 각 이동통신사는 이미 가입하여 이용하는 서비스를 위해 보유하고 있는 개인정보에 대하여 정보주체의 검색・저장・유통이 가능하도록 플랫폼을 구축하여 각종 구비서류 대신 꼭 필요한 데이터만 군장병이 요청 할 경우 이동통신사에 전송할 수 있도록 개인정보 관리 전문기관을 운영하는 것을 제안한다.



(그림 1) 개인정보관리 전문기관을 통한 군장병 휴대전화 개통 처리

(Figure 1) Opening of mobile phones for service members through personal information management organizations

이와같이 통신분야 마이데이터 체계를 구축하게 되면 통신대리점은 개인정보 처리 등에 신경쓰지 않고 통신서비스 상품에만 집중할 수 있고, 이동통신사는 개인정보 처리자 즉 위탁업무를 처리하는 통신대리점에서 위탁업무를 처리하는 과정에서 위법하게 개인정보를 수집하거나 위탁목적외로 활용하는 것에 대한 관리・감독 비용감소로인해 통신서비스 강화에 더욱 집중할 수 있다.

또한, 군장병은 자신의 개인정보를 최소한으로 제공하면서도 원활한 통신서비스의 가입 등 편의와 신뢰성을 확보할 수 있는 환경을 제공할 수 있다.

5.2.4 관련 법규 및 문제점 해결방안

전기통신사업법 제32조의4제4항 “본인임을 확인할 수 있는 증서 및 서류의 종류 등에 필요한 사항은 대통령령으로 정한다”라고 정하며 동법 고시 제37조의6제2항 제1호 “개인:주민등록증, 운전면허증, 국가유공자증, 독립유공자증, 5・18민주유공자증 또는 대한민국 여권”으로 그 정서를 한정하고 정보통신망을 이용하여 계약을 체결하는 경우 전자서명을 통한 확인으로 대체할 수 있음을 정하며 부정가입방지시스템을 이용하여 각 증서의 진위확인을 하도록 강제하고 있다.

개인정보보호법 제24조의2제1항제2호 “정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우” 혹은 같은 항 제3호 “주민등록번호 처리가 불가피한 경우로서 개인정보보호위원회가 고시로 정하는 경우” 등으로 정하고 있다.

따라서, 개인정보 관리 전문기관의 인허가를 위해 전기통신사업법 상의 본인임을 확인할 수 있는 명시적인 방법이 대통령령에 포함되도록 법률 개정이 잇따라야 하며, 개인정보보호법 개인정보보호위원회의 고시에 개인정보의 제공사항이 포함되어 그림 1과 같이 개인정보관리 전문기관을 통한 군장병 휴대전화 개통 환경을 구축한다면 통신대리점 및 재위탁점의 사용인・종업원 등은 이동통신사가 통신대리점에게 제공한 정보 및 제공된 정보를 가공・복제・조합 하는 방법을 포함하여 모든 개인정보를 위법하게 활용할 수 있는 수단을 원천적으로 차단하여 개인정보 불법활용을 최소화 할 수 있을 것이다.

5.3 군장병 개인정보 실태점검 지속 시행

5.3.1 군장병 휴대전화 사용에 따른 개인정보 보호

국방부는 군장병의 생활안정과 복지증진에 이바지하고자 군인공제회 수익사업 등을 통해 복지혜택을 제공하고 있다. 그중에서 군장병 휴대전화 이용시 각종 복지혜택을 제공하기 위하여 이동통신사로부터 위탁계약을 체결하고 단말기 할인 및 요금할인 등을 제공하며 군장병의 가입신청업무를 맡고 있다. 이동통신사가 위탁업무에 대해 개인정보보호 실태점검 등을 수행하고 있듯이 군 자체에서도 군장병의 개인정보를 처리하는 현장에 대한 지속적인 현장점검 및 개인정보보호 교육 등의 관리・감독을 지속할 필요가 있다.

6. 결 론

본 연구의 목적은 군장병이 휴대전화 개통신청을 할 때마다 매번 개인정보 수집 행위를 하는 것이 아니라 기

존에 가입하여 이용 중인 서비스에 대해 각 이동통신사가 보유하고 있는 개인정보를 활용하여 본인확인 절차만 거쳐 개통이 이뤄어진다면 통신대리점은 직접적인 개인정보 수집 행위 자체를 제한할 수 있을 것이다.

본 연구에서 제시한 개인정보관리 전문기관을 통해 군장병이 휴대전화 개통시 개인정보 이동권을 이용하여 요청한 정보주체의 개인정보를 검색・저장・유통이 가능하도록 플랫폼을 구축할 경우 통신대리점 및 재위탁점의 사용인・종업원 등이 군장병의 개인정보를 위법한 방법으로 수집・이용 할 수 있는 수단을 원천적으로 차단하고 개인정보 안정성을 확보할 수 있을 것이다.

참고문헌(Reference)

[1] "2020 Defense White Paper", Ministry of National Defense, Republic of Korea, pp. 272-275, 2020.

[2] "2022 National Information Protection White Paper," National Intelligence Service, Ministry of Science and ICT, Ministry of Public Administration and Security, Personal Information Protection Committee, Ministry of Foreign Affairs, pp. 35~43, 2022. https://www.kisa.or.kr/public/library/etc_View.jsp?regno=0238&searchType=&searchKeyword=&pageIndex=1

[3] Gi Pyong-gi, "Progress and Significance of Daily and Post-Cell Phone Use System", Korea National Defense Institute, Defense Issue Briefing Series, 2020-14.

[4] Deliberation and resolution of the Personal Information Protection Committee "A matter concerning the use of personal information by military personnel for the installation of the Ministry of National Defense's illegal gambling prevention program", No. 2021-105-009, March 24, 2021.

[5] Choi Kyung-jin, "2020 EU General Personal Information Protection Act Guidebook", Korea Communications Commission & Korea Internet & Promotion Agency, pp. 19-21. https://gdpr.kisa.or.kr/gdpr/bbs/selectArticleList.do?bbsId=BBSMSTR_000000000101

[6] Lee Jae-sung & Kang Hye-young, "2019 Personal Information Protection Counseling Casebook," Korea Internet & Security Agency, KISA-2020-0008, pp. 18~19, 2020. https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS233&mCode=D070010030#

[7] Joint measures by the relevant ministries, "Medium-to-Medium-Term Comprehensive Measures for Intelligent Information Society in Response to the Fourth Industrial Revolution", Press Release 2016.12.27.

[8] Ministry of Public Administration and Security, "My information held by administrative and public institutions is directly controlled and utilized by <I directly control and utilize> Ministry of the Interior and Safety's My Data Project," press release. 2020.6.24.

[9] Jeong Min Choi & Youngeun Jo, "A Study on the Right to Data Portability and MyData Industry", Journal of Law & Economic Regulation, Vol. 13, No 2, pp. 92~107, 2020-11. http://data.doi.or.kr/10.22732/CeLPU.2020.13.2.92

◐ 저 자 소 개 ◑

황 보 원 규(Wongyu Hwangbo)
1998년 동국대학교 DUICA(2007년 학점은행제 정보보호학과(공학사))
2011년 고려사이버대학교 정보관리서비스학과(정보학사)
2013년 성균관대학교 대학원 정보보호학과(공학석사)
2021년~현재 세종대학교 대학원 컴퓨터공학과(박사과정)
관심분야 : 정보보호, 개인정보보호, 머신러닝, 인공지능, 정책제도개선, etc.
E-mail : goldhbwk@gmail.com

신 동 규(Dong-kyoo Shin)
1986년 서울대학교 컴퓨터과학과(공학사)
1992년 Illinois Institute of Technology 대학원 컴퓨터과학과(공학석사)
1997년 Texas A&M University 대학원 컴퓨터과학과(공학박사)
1998년~현재 세종대학교 컴퓨터공학과 교수
관심분야 : 사이버전, 사이버보안, 사이버 지휘통제, 인공지능, 정보보호, etc.
E-mail : shindk@sejong.ac.kr