우리나라의 개인정보 침해 실태와 한국우정의 대책

이 용 수*

개인정보는 개개인의 내외면, 사회관계, 권리를 나타내는 인권적인 가치와 고객의 정보를 수집 활용하여 영업 활동 및 수익을 창출하는 기업의 영영자산이 되기도 한다. 또한 공공 민간 서비스, 기업경영 등 대부분의 사회 활동이 개인정보를 기반으로 이루어짐으로 사회의 중요한 요소이기도 하다. 이러한 개인정보가 비즈니스적인 가치의 증가와 다양한 개인정보의 수집처가 존재하고 디지털 개인정보의 무한 복제 및 빠른 전파성은 개인정보의 가치 및 디지털 기술의 특성 등으로 인해 개인정보의 노출기회가 많아지고 유출 위험도 지속적으로 증가하고 있다.

개인정보침해신고센터에 접수된 상담 및 신고 접수 현황은 2013년 기준으로 175,389건으로 나타나고 있다.

이러한 신고건수는 새로운 기기(스마트폰 등) 및 서비스(클라우드, SNS 등)의 확산과 개인정보 유출사고, 이용자의 개인적인 정보에 대한 관심 증가로 인해 개인정보침해건수는 향후에도 증가 할 것으로 예상되고 있다.

2014년 1월에 발생한 신용카드사의 개인정보 유출과 관련해서 집단소송을 제기하지 않은 피해자들에게도 정신적인 위자료를 지급해야 된다는 입장에서 국민은행, 하나로 텔레콤 등은 최소 10만원에서 30만원까지 정신적 고통에 따른 위자료를 지급해야 된다는 법원의 판결이 있었다.

만약 법원에서 신용카드사 개인정보 유출에 대한 위자료를 인정했다고 할 경우 1억 건의 정보유출에 20만 원씩의 위자료를 인정하면 배상액이 20조 원에 달해 기업의 존폐를 결정지을 수 있는 중요한 요소가 될 것이다.

본고에서는 과거에 비해 개인정보에 대한 인식과 법/제도에서 강화되고 있는 개인정보에 대하여 전반적으로 정리하고자 한다. 이를 위해 우선 개인정보의 정의 및 유형, 해외의 개인정보 보호 대책, 우리나라의 개인정보 침해 실태를 살펴보고 한국우정은 개인정보 침해에 대비하여 어떠한 대책을 가지고 있는지 살펴본다.

Ⅰ. 개인정보의 정의 및 유형

ICT가 급속적으로 발전하면서 사회 각 분야에서 인터넷과 정보통신기술의 사용이 일상화되

* KISDI 우정경영연구소 부연구위원, yongsoo@kisdi.re.kr

고 금융거래 등 사회의 구성, 유지 발전을 위한 필수적인 요소로 개인 정보가 부각되고 있다.

개인정보란 개인의 신체, 재산, 사회적 지위, 신분 등에 관한 사실, 판단, 평가 등을 나타내는 일체의 모든 정보를 말한다.

우리나라의 "정보통신망이용촉진 및 정보보호 등에 관한 법률"에서는 개인정보를 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아 볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보로 정의하고 있다.

일본의 개인정보보호법에서 개인정보는 생존하는 개인에 관한 정보로서 특정한 개인을 식별할 수 있는 정보(다른 정보와 쉽게 대조하여 특정한 개인을 식별할 수 있는 정보를 포함한다)를 의미한다.

〈표 1〉 개인정보 유형

구 분	개인정보유형
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술 자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물
소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
기타수익정보	보험(건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납건수, 임금압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트결과, 직무태도
법적정보	전과기록, 자동차교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(e-mail), 전화통화내용, 로그파일(log file), 쿠키(coo-kies)
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

이러한 개인 정보 유형은 앞의 〈표 1〉과 같이 다양하게 구분 할 수 있다.

개인 정보의 가장 일반적인 유형은 일반정보로 이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적을 인식할 수 있는 정보이며, 가족정보는 가족 구성원들의 이름이나 출생지 등과 관련된 정보이다. 그리고 이외에도 소득정보, 신용정보, 의료정보, 조직정보, 위치정보, 신체정보, 습관 및 취미정보 등 우리가 일상에서 무시하거나 소홀히 다루었던 개인과 관련된 다양한 정보 유형이 있다.

이러한 개인정보는 〈표 2〉와 같이 현대사회에서 다양하게 이용되고 있다. 예로 증명서를 발급받을 때 보통 이름, 연락처, 주소, 가족관계, 소득, 세금 납부수준 등을 기재하고, 건물의 출입통제 할 때는 이름, 연락처, 방문목적 등을 기재하고 있다.

〈표 2〉 개인정보의 이용 실태(예시)

구분	개인정보
인터넷 쇼핑	– 이름, 연락처, 주소 – 결제계좌번호 – 카드번호
증명서 발급	– 이름, 연락처, 주소 – 가족관계 – 소득, 세금
건물 출입 통제	– 이름, 연락처, 주소 – 주민등록번호 – 출입기록(시간, 위치)
콜 센터	– 이름, 연락처, 주소 – 결제 또는 카드번호, 구매물품 정보 – 카드번호, 결제정보
교통카드 결제	– 카드번호, 이름 – 주민등록번호 – 결제정보, 위치정보
가입신청	– 이름, 주민등록번호 – 연락처, 주소, 메일주소 – 결제계좌 번호

개인정보는 정보기술과 결합하여 개인정보의 활용이 확대되고 있다. 쇼핑센터에서는 온라인 상품검색, 결제, 배송서비스를 제고할 수 있으며, 영화관에서는 인터넷, 모바일로 예매를 하고 무인발권시스템도 운용하고, 주택관리업에서는 홈 네트워크 관리시스템을 통해 보다 효율적인 주택관리를 하는 등 다양한 영역에서 순 방향적인 이용이 있는 반면, 대부분의 정보가 정보시스템으로 처리됨에 따라 시스템에서 일부 사고가 사회 전체에 영향을 미치면서 피해범위도 확대되고, 인터넷/게임중독/반사회적 유해 매체 범람, 사이버 명예훼손 등 다양한 정보화의 역기능이 출연하고 있으며, 개인정보가 대량으로 수집, 이용되기 시작하면서 개인정보의 유출, 침해행위도 크게 증가하는 역방향적인 현상도 나타나고 있다.

Ⅱ. 외국의 개인정보 보호 대책

1. 유럽연합(EU)의 개인정보 보호 대책

유럽연합은 최근 데이터 관리자의 정당한 이익 추구에 대한 개인 정보 이용을 허용하고 있는 'EU 개인정보보호 지침'에 관한 혼란을 방지하기 위해 이를 보다 상세히 규정한 가이드라인을 공개하였다.

가이드라인은 6개의 판단 기준을 제시하고 데이터 관리자가 그 중 한 개 이상의 기준을 충족시킬 경우 적법성을 확보하고 있다고 명시하였으며, 이익 추구 활동의 정당성을 판단하기 위해 이용자의 개인 정보와 데이터 관리자의 이익을 상호 측정하기 위한 '균형성 테스트'를 제안하고 있다.

EU의 개인정보보호 정책 자문조직 'Article 29 Working Party(WP29)'는 'EU개인정보보호지침' 제7조에서 규정한 '정당한 이익(Legitimate Interest)'에 관한 가이드라인을 2014년 4월 9일 발표하였다. 제7조는 정당한 이익이 있을 시 데이터 관리자들의 개인정보 이용을 허용하고 있으며, WP29는 제7조 관련 '정당한 이익'의 해석과 운용을 놓고 서로 다른 의견과 판단이 제기되는 것을 방지하기 위해 가이드라인을 마련하고, 가이드라인은 개인의 프라이버시 보

호와 데이터 관리자의 정당한 이익 간 균형성 테스트를 이행하기 위한 절차로 구성되어 있다.

이러한 가이드 라인의 주요 내용은 첫째 데이터 관리자(정부, 기업, NGO 등)가 개인정보를 취급 할 때 최소한 아래 6개 항목 중 하나 이상을 충족했을 경우 적법성을 확보한 것으로 판단한다.

1. 데이터 주체인 개인의 분명한 동의
2. 데이터 주체와의 계약 실행
3. 데이터 관리자에게 부과되는 법적인 의무의 준수
4. 데이터 주체의 핵심적인 이익의 보호
5. 공공의 이익을 위해 필요한 업무의 실행
6. 데이터 관리자의 '정당한 이익'

'정당한 이익'은 EU와 회원국 법률에 합당하고, 〈표 3〉과 같이 균형성 테스트를 충분히 거쳐야 이행 가능하며 이행 시 데이터 처리자의 투명성과 책임성에 대해 강조하고 있다.

〈표 3〉 균형성 테스트 단계

단 계	내 용
1	제7조의 법적인 적용 여부
2	이익의 정당성 또는 비정당성 여부 판단
3	이익의 관철을 위해 데이터 처리 절차가 필요한 지 여부 판단
4	데이터 관리자의 이익이 데이터 주체의 기본권에 의해 거부되는 지 여부 판단
5	추가적인 구제수단의 제공 여부
6	컴플라이언스의 실현과 투명성의 확보
7	데이터 주체의 거부권 행사 여부

균형성 테스트 시 핵심 고려 사항은 다음과 같다.

1. 데이터 관리자의 정당한 이익의 평가
2. 데이터 주체에게 주는 영향

3. 법률적 균형

4. 데이터 주체에게 주는 부정적 영향 방지를 위한 데이터 관리자의 추가적인 구제수단 확보

WP29는 이번 가이드라인을 통해 EU 회원국들이 '정당한 이익'과 균형성 테스트의 개념을 공유해야 한다고 강조하면서 EU 데이터보호법(EU General Data Protection Regulation)에 반영되고 데이터 관리자의 책임에도 반영되어야 한다고 밝히고 있다.

2. 일본의 개인정보 보호 대책

일본은 2003년 개인정보보호법을 제정하였으나, 2013년 12월 20일에 개인정보의 활용에 관한 제도 재검토 방침을 결정하여 2014년 6월에 개인정보보호법 개정초안의 골자를 공표하였다.

이는 개인 데이터의 이용가치가 점차 높아지면서 개인정보보호법 제정 당시에는 예상하지 못했던 개인정보 및 프라이버시에 관한 사회적 상황이 현행법 제정 당시와는 변화하고 있는 것을 반영하기 위한 절차로 보여진다.

개인정보보호법 개정초안에서 밝히고 있는 이번 제도 개정의 배경은 다음과 같다.

첫째는 개인정보의 이용 가치가 높아지고 있으나 보호해야 할 정보의 범위와 사업자가 준수해야 할 규칙은 불분명하다는 것이며, 둘째는 지금까지 보다 충분한 주의를 기울여 개인 데이터를 취급해 달라는 소비자 의식도 확대되고 있는 점을 감안하여 개인 데이터가 적정하게 취급되는 것을 분명히 하고 소비자를 안심시키는 제도 구축이 요구되고 있다는 시대적인 흐름의 반영이다. 그리고 셋째는 개인정보와 프라이버시 보호를 도모하면서 신산업・신서비스의 창출 등을 위해 활용할 수 있는 환경 정비가 요구되고, 넷째는 외국의 정보 이용・유통 및 프라이버시 보호 모두를 확보하기 위한 대응을 꾀하고 있는 점을 감안 할 때 개인정보보호 관련 제도의 국제적인 조화를 도모할 수 있도록 국제적 수준의 개인정보보호 제도를 마련할 필요가 있다는 것이다.

새로운 개정초안의 핵심 포인트는 세 가지로 볼 수 있다. 첫째는 정부가 독립적인 개인정보보호 전문기관을 설치하여 일본의 개인정보보호제도를 국제수준에 맞추는 것이다. 이번 개인정보보호법 개정초안의 핵심 중 하나는 개인정보보호에 관한 지침 작성과 행정 처분 등을 실시하는 제3자 기관의 설립을 담고 있다는 점이다. 이 기관은 공정거래위원회 또는 국가공안위원회와

법적으로 대등한, 정부의 행정조직으로부터 독립적인 개인정보보호를 위한 기관이 될 것이다.

둘째는 기업의 자율규제 규칙을 지지하고, 기술이 발전함에 따라 확대된 "개인정보"의 회색지대를 해소하는 것을 목표로 한다. 개인의 권리 이익의 보호와 사업활동의 실태를 배려하면서, 지문인식 데이터, 얼굴인식 데이터 등 개인의 신체적 특성에 관한 것 중에서, 보호 대상이 되는 것을 명확히 하고, 필요에 대응하여 규율을 정하도록 하는 것이다. 보호대상이 되는 "개인정보" 등의 정의에 해당하는지 여부에 대해 제3자 기관이 해석의 명확화를 도모하는 것과 동시에, 개별사안에 대한 사전 상담 등에 신속히 대응하도록 한다.

셋째는 개인 식별을 어렵게 한 후 그 데이터를 타사에 전달하여 활용할 수 있도록 규제를 완화하는 것이다. 정부는 개인과 관련된 데이터이면서도 특정 개인을 식별할 수 없도록 하여 그 권리와 이익을 침해하지 않는 데이터를 활용한 새로운 사업의 창출을 생각하고 있다.

프라이버시 보호와 기업의 개인정보 활용 강화라는 목적은 올바르게 보여지나, 보호될 데이터의 정의가 아직 불명확하며, 제3자 기관의 실효성도 불투명한 실정이다. 개정초안에서는 지문인식 데이터, 얼굴인식 데이터 등 개인의 신체적 특성에 관한 것 중에서 보호대상을 명확히 한다고 하였으나, 산업계가 난색을 표한 인터넷 검색 기록이나 구매 이력, 스마트폰의 위치정보 등도 향후 법제화 과정에서 계속적으로 검토가 이루어 질 것으로 보인다.

Ⅲ. 우리나라의 개인정보 침해 실태

우리나라의 대규모 개인정보 침해 사례를 보면 〈표 4〉와 같이 1억건 까지도 발생하는 등 규모가 커짐을 볼 수 있다.

2008년에는 옥션과 하나로텔레콤, GS칼텍스가 600만명에서 1,800만명까지 피해규모가 나타났으며, 2011년에 SK컴즈에서 발생한 3,560만명의 대량 유출사고가 발생했다. 그러나 2012년과 2014년에 카드사들에서 1억건 이상의 개인정보 유출사태가 발생하면서 사회에 큰 충격을 주면서 개인정보에 대한 인식이 변화되는 전환점을 맞이하였다.

〈표 4〉 대규로 개인정보 침해 사례

발생일	발생기업	피해규모
2008. 2	옥션	1,800만명
2008. 4	하나로텔레콤	600만명
2008. 9	GS칼텍스	1,150만명
2010. 3	신세계몰 등 25개 업체	2,000만명
2011. 4	현대캐피탈	175만건
2011. 5	리딩투자증권	12,000건
2011. 5	세티즌	140만명
2011. 6	대부업체, 저축은행, 채팅사이트	1,900만건
2011. 7	SK컴즈(네이트, 싸이월드)	3,560만명
2011. 8	삼성카드	47만건
2011. 11	넥슨	1,320만건
2012. 5	EBS	400만건
2012. 7	KT	870만건
2012. 12	BC카드, 국민카드ISP시스템	18,000만건
2014. 1	KCB, NH카드, 롯데카드, 국민카드	10,400만건

우리나라의 개인정보 침해 신고 및 상담건수는 매년 증가하는 양상을 〈표 5〉와 같이 보이고 있다. 2011년에 가장 증가한 67,383건이 상담되었으며 2013년에 다소 증가폭이 주춤하는 양상이 보이고 있다. 이는 과거에 비해 개인정보에 대한 인식과 법 제도가 정비되면서 점차 개인정보에 대한 관리가 강화되면서 나타나는 것으로 생각된다.

〈표 5〉 연도별 개인정보 신고 상담 건수 추이

연도	상담건수	증감
2013	177,736	10,935
2012	166,801	44,586
2011	122,215	67,383
2010	54,832	19,665
2009	35,167	−4,644

연도	상담건수	증감
2008	39,811	13,846
2007	25,965	2,632
2006	23,333	5,127
2005	18,206	637
2004	17,569	-208
2003	17,777	17,777

개인정보침해센터에 접수된 개인정보의 접수유형을 보면 2013년에 신고된 신고 상담 건수는 177,736건으로 집계되었다. 이중 신고 건수는 2,347건이고 상담 건수는 175,389건이다.

이를 접수 유형별로 분석하면 〈표 6〉과 같다.

〈표 6〉 개인정보 접수 유형

접 수 유 형	2013년
이용자의 동의 없는 개인정보 수집 관련	2,634
개인정보 수집시 고지 또는 명시 의무 관련	84
과도한 개인정보 수집	1,139
목적 외 이용 또는 제3자 제공 관련	1,988
개인정보 취급자에 의한 훼손·침해 등	1,022
개인정보 처리 위탁 시 고지의무	44
영업의 양수 등의 통지의무	47
개인정보관리책임자 관련	51
기술적·관리적 조치 미비 관련	4,518
수집 또는 제공받은 목적 달성 후 개인정보 미파기	602
동의철회·열람 또는 정정 요구 관련	674
동의철회, 열람·정정을 수집보다 쉽게 해야 할 조치	510
아동의 개인정보 수집	36
주민등록번호 등 타인 정보의 훼손·침해·도용	129,103
정보통신망법 적용대상 외 관련(신용정보 관련 문의 등)	35,284
합 계	177,736

개인정보 접수유형 중 주민등록번호 등 타인 정보의 훼손/침해/도용이 전체의 73%로 가장 많이 나타났으며 다음으로 정보통신망법 적용 대상 외 관련(신용정보 관련 문의 등)이 20%로 나타났다. 또한 다음으로 기술적·관리적 조치 미비 관련 4,518건으로 나타났으며, 다음으로 이용자의 동의 없는 개인정보 수집 관련이 2,634건으로 집계되었다.

〈표 7〉 2014년도 월별 개인정보침해신고 상담건수

구분	1월	2월	3월	4월	5월	6월	7월
이용자의 동의없는 개인정보 수집	261	240	261	410	1,060	630	275
개인정보 수집시 고지 또는 명시 의무 불이행	14	2	210	7	7	5	3
과도한 개인정보 수집	71	137	146	80	86	105	90
고지·명시한 범위를 넘어선 이용 또는 제3자 제공	146	132	166	211	171	183	228
개인정보 취급자에 의한 훼손·침해 또는 누설	179	99	69	76	50	70	83
개인정보 처리 위탁시 고지의무 불이행	5	4	9	5	2	2	1
영업의 양수 등의 통지의무 불이행	3	6	8	8	1	5	8
개인정보관리책임자 미지정	1	5	4	2	4	6	2
기술적·관리적 조치 미비로 인한 개인정보누출 등	238	264	1,037	696	258	298	443
수집 또는 제공받은 목적 달성 후 개인정보 미파기	47	65	54	69	32	26	74
동의철회·열람 또는 정정 요구 불응	69	58	69	52	106	54	63
동의철회, 열람·정정을 수집보다 쉽게 해야할 조치 미이행	49	29	28	34	23	21	37
법정대리인의 동의없는 아동의 개인정보 수집	4	1	1	3	4	3	4
주민등록번호 등 타인 정보의 훼손·침해·도용	10,642	4,056	6,914	6,141	4,976	5,399	6,900
정보통신망법 적용대상 이외의 개인정보침해(신용정보침해 등)	4,673	6,530	4,049	3,900	3,633	4,040	5,584
합계	16,402	11,628	13,025	11,694	10,413	10,847	13,795

2014년에 개인정보 침해 신고 상담건수는 앞의 〈표 7〉과 같이 월별로 만건이상으로 나타나고 있다. 2013년에 실적에서도 가장 많은 건수를 보인 주민등록번호 등 타인 정보의 훼손/침해/도용과 정보통신망법 적용대상 이외의 개인정보침해(신용정보침해 등)에서 많이 발생되고 있음을 알 수 있다.

2013년에 한국인터넷진흥원에서 발표한 2012년 개인정보 보호 상담 사례집에서는 개인정보 보호에 대한 상담 사례를 정리하여 발표하고 있다. 본 보고서에서는 개인정보 수집·이용, 개인정보 제3자 제공, 처리위탁 및 영업양도, 민감정보 및 고유식별 정보 처리, 개인정보 관리체계, 개인정보 파기, 정보 주체 관리, 영상정보처리기기(CCTV) 등으로 나누어서 발표를 하고 있다. 이 중에서 개인정보 수집·이용, 개인정보 안정성 확보조치, 개인정보 관리체계 중심으로 정리를 한다.

개인정보 수집·이용과 관련한 몇 가지 사례를 정리하면 다음의 〈표 8〉과 같다.

〈표 8〉 개인정보 수집·이용과 관련한 사례

관련 영역	질문	답변
공공/민간	병원에서 초진 환자의 개인정보 수집 시 동의 취득 여부는	의료기관의 의료법에 따라 수집하는 개인정보는 정보주체의 동의 없이 수집 가능하나 홍보 등과 같이 의료행위와 직접 관계가 없는 경우에는 동의를 받아야 한다.
공공/민간	기업에서 입사지원을 받기 위해 수집할 수 있는 최소한의 개인정보의 범위, 입사지원서 접수 시 개인정보 수집 동의를 받아야 하는지	직원 채용 단계에서 지원자 확인 및 연락에 필요한 성명, 전화번호, 주소 등과, 직무수행 능력을 평가하기 위한 학력, 성적, 자격사항 등이 필요 최소한의 정보가 될 수 있다. 직원채용에서 수집되는 정보는 지원자의 동의 없이 수집·이용 할 수 있다.
민간	금융회사의 전화 상담 시 주민등록번호 입력을 요구하는 경우 문제가 없는지	전화 ARS 상담 시 무조건적으로 주민등록번호를 입력하도록 하는 것은 과도한 개인정보 수집의 우려가 있다.
공공	구청에서 장애인 지원비용을 신청하는 과정에서 각종 진료비 명세, 금융계좌 등 상세한 개인정보를 수집하는데 동의를 받지 않아도 되는지	'공공기관의 법령에서 정하는 소관업무 수행을 위해서 개인정보를 수집하는 경우'에는 동의를 요하지 않는다.

개인정보 안정성 확보 조치와 관련한 몇 가지 사례를 정리하면 다음의 〈표 9〉와 같다.

〈표 9〉 개인정보 안정성 확보조치 사례

관련 영역	질문	답변
민간	인터넷 공동구매 관리자가 개인정보 명단을 노출한 경우 개인정보 유출인지	블로거는 개인정보 처리자에 해당하므로 개인정보가 분실, 도난, 유출, 변조, 훼손되지 않도록 필요한 조치를 취할 의무가 있다.
공공/민간	인터넷에서 개인정보가 모두 조회 가능한 관리자메뉴가 공개되는 경우 어떠한 조치를 해야되는지	개인정보처리자는 개인정보가 열람권한 없는 자에게 공개되거나 외부에 유출되지 않도록 조치를 취하여야 하고 구체적으로 인터넷 웹사이트 등을 통하여 개인정보 노출이 발생되지 않도록 하여야 한다.

개인정보 관리체계와 관련한 몇 가지 사례를 정리하면 다음의 〈표 10〉과 같다.

〈표 10〉 개인정보 관리체계와 관련한 사례

관련영역	질문	답변
공공/민간	개인정보 보호 책임자가 퇴사한 후에도 이를 수정하지 않은 경우 어떻게 해야되는지	개인정보 보호책임자를 지정하고 공개하는 경우에는 그 변경사항을 빠짐없이 반영하여야 한다.
민간	기업에서 모기업, 계열사 모두 개인정보 보호 책임자를 지정해야 되는지	기업집단에 속한 계열사라 하더라도 그 사업목적과 범위, 개인정보의 처리목적이 각각 상이한 경우에는 계열사 마다 각각 개인정보 보호책임자를 지정하여야 한다.

Ⅳ. 한국우정의 개인정보 보호 대책

한국우정은 안전한 정보보호 기반 강화를 위해 지능화・고도화되는 사이버 위협에 대비하여

관리적·기술적 정보보호 관리체계 강화를 통해 대국민 우정서비스 신뢰성을 강화하고자 노력하고 있다.

이를 위해 우정사업 고객정보보호의 무결점·무사고 달성을 개인정보보호 목표로 하여 정보반출입 관리시스템 구축, 정보수집, 보유 기준 마련, 전직원 사이버 교육 실시, 정보시스템 접근제한 등 다양한 전략을 추진하고 있다.

국가정보원에서 배포된 PC보안 점검프로그램 『내PC지킴이』는 점검항목에 대한 실행결과 분석 및 통계관리에 어려움이 있어, 기존 『내PC지킴이』의 기능에 추가적으로 관리가 필요한 점검항목을 통합하여 PC보안점검 프로그램을 자체 개발할 예정이다. 점검항목은 〈표 11〉과 같이 19개 항목으로 확대하여 보안을 강화 할 것이다. 이를 통해 우본 직원과 외부용역 직원에 대하여 보안진단 항목을 확장하여 점검함으로써 사용자 PC의 보안의식 및 정보보호수준을 강화하고 최적의 PC보안 상태를 유지함으로써 내부자료 유출에 대해 사전 차단이 가능하게 하도록 할 예정이다.

〈표 11〉 PC보안 점검 항목

구 분	항 목
보안프로그램(7)	PC보안관리Agent, 백신프로그램 설치, 백신프로그램 엔진업데이트, 백신프로그램 실시간감시, 문서보안Agent, 보조기억매체제어 Agent, 개인정보 자가진단프로그램 설치
보안환경(12)	화면보호기 설정, PC내 공유폴더 설정, 윈도우 로그인 암호설정, PC내 다중네트워크 설정, 컴퓨터 식별번호 현행화, 웹공유 프로그램사용, 한글프로그램 최신보안패치, 로그인비밀번호 안전성 여부, 로그인비밀번호 변경, USB자동실행 허용여부, Guest계정 활성화 여부, 개인정보자가진단 점검결과

경영·우편시스템의 고객정보를 보호하기 위한 문서보안시스템 성능개선 사업을 추진 할 예정이다. PC운영체제 Windows7 문서보안 기능 구현(Windows8 지원가능)하고, 기존 업무용 소프트웨어 및 최신의 소프트웨어까지도 암·복호화하며, 기 연동(우편물류시스템, 전자결재 등)되어 있는 문서보안 적용대상 시스템에 대한 안정적 연계를 이루도록 할 예정이다. 또한 정보유출방지를 위하여 외부저장매체(USB 등) 통제관리 기능을 구현하고, 사용자의 문서접근

(열람/저장/편집) 이력정보 관리를 함으로써 고객정보에 대한 보호를 강화할 것이다.

기존의 정보보호관리시스템을 고도화 시킬 예정이다. 정보보호 운영관리와 정보유출통합관리 시스템의 기능 통·폐합 및 노후장비를 교체하고 인터넷 사용량 증가에 따라 정보유출방지시스템 저장 공간 확대를 통해 6개월 이상 보관 가능토록 기능 개선할 것이다.

또한 단위 정보보호시스템(좀비PC탐지, 무선침입방지, 우체국금융 후선업무 DB접근제어, 금융고객조회이력관리시스템 등)의 보안로그를 추가 연계할 것이며, 정보유출방지를 위한 탐지·분석 정책을 고도화하여 내부정보 오·남용 사용 예방 및 관리체계 구축과 다양한 경로를 통한 정보사용 이력기록 및 종적관리가 이루어 지도록 할 것이다.

다량의 개인정보 유출사고 및 해킹·피싱 등 정보시스템의 지속적 위협 등에 대응한 우정사업의 정보보안 전문인력 육성으로 정보보안의 강화를 추진 할 예정이다. 정보보안 전문자격증을 취득하도록 하고, 우본, 정보센터, 서울청 등에 전문 인력을 배치 추진하며, 정보보안 전문인력 관리를 위해 정보화 부서(우편, 금융 정보화 및 정보보안 부서)에 정보보안 자격 취득자 배치로 시스템 개발·관리·운영 시 정보보안 강화하고 정보보안부서 근무자의 정보보안 자격 취득을 적극 지원(교육, 수험료 등)할 예정이다.

우정사업의 개인정보 보호 체계 점검과 이미지 제고를 위해 개인정보보호법(13조)에 따라 기관의 개인정보 보호 체계를 대내·외 공증하는 개인정보 보호 인증(PIPL: Privacy Information Protect Level)을 추진할 것이다.

개인정보 보호 인증(PIPL)은 개인정보보호법의 도입 취지에 따라 개인정보처리자의 개인정보 보호 관리체계 구축 및 개인정보 보호조치 사항을 이해하고 일정한 보호수준을 갖춘 경우 인증 마크를 부여하는 제도이다.

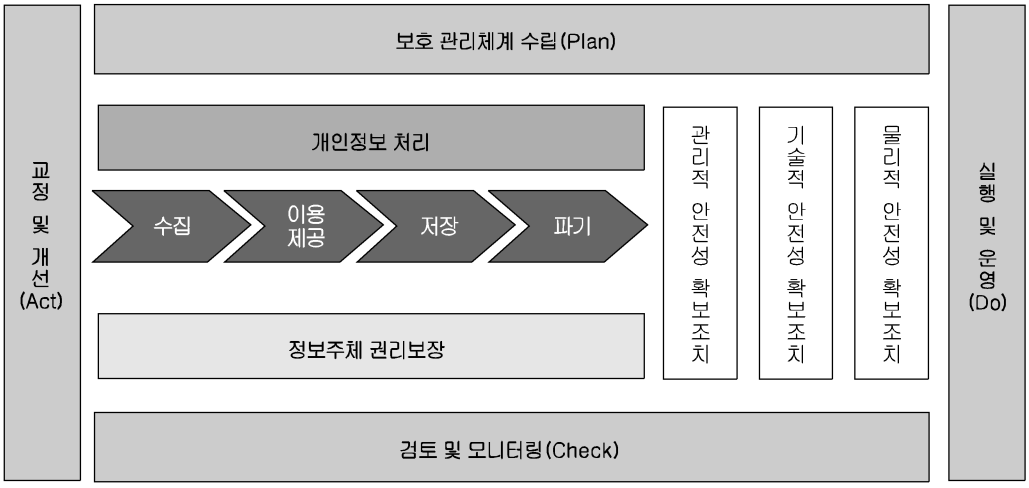
개인정보 보호 인증의 적용대상은 업무를 목적으로 개인정보를 처리하는 공공기관, 민간기업, 법인, 단체 및 개인 등 모든 공공기관 및 민간 개인정보 처리자를 대상으로 한다.

개인정보 보호 인증과정을 통한 기대효과는 개인정보 보호 관련 법령에서 요구하는 기준을 우정사업본부 내부에서 준수하는지 여부를 점검하고, 조직 내부 구성원에게 개인정보 보호에 대한 중요성을 전파하여 정보보호 인식 및 역량을 제고하게 될 것이다. 또한 정보보호 인증취득에

따라 안전행정부에서 제공하는 다양한 혜택을 받을 수 있는 장점이 있다.

〔그림 1〕 PIPL 혜택 및 관리체계

「개인정보 보호 인증제 운영에 관한 규정」에 따른 근거
제28조(인증취득기관의 혜택) ① 안전행정부장관은 인증취득기관에서 「개인정보보호법」에 따라 실시하는 기획점검 대상 제외 또는 실시 유예, 행정처분 감경 등의 혜택을 줄 수 있다. ② 안전행정부장관은 인증취득기관에게 개인정보 보호 우수기관 포상, 개인정보 보호 인증 관련 교육기회 및 정보제공, 행사 참여기회 제공 등의 혜택을 줄 수 있다.



'개인정보 보호 관리체계' 분야는 PDCA(Plan-Do-Check-Act)의 관점에서 '보호체계 수립(Plan)', '실행 및 운영(Do)', '검토 및 모니터링(Check)', 그리고 '교정 및 개선(Act)'으로 심사영역으로 구성되어 있으며, '개인정보 보호대책' 분야는 '관리적, 기술적, 물리적 안전성 확보조치' 등과 같은 보호조치 뿐 만 아니라 법적으로 요구되는 '개인정보 처리', '정보주체 권리보장' 등에 대한 항목을 포함하여 심사영역이 구성되어 있다.

현재 본부에서만 운영되고 있으나, 지방체신청까지 무선 침입 방지 시스템을 확산 할 예정이다.

구내 비인증 무선 네트워크의 탐지 및 차단, 무선 AP에 대한 외부 불법 접속 탐지 및 차단 등 무선망 보안을 강화하고 외부의 불법 접속 뿐 만 아니라, 부내에서 발생할 수 있는 스마트폰

핫스팟 탐지, 인가 받지 않은 인터넷 공유기 사용 등도 탐지 할 수 있게 할 필요가 있다.

우편분야에서 우편보안담당자가 전 시스템의 개인정보를 통괄적으로 관리할 수 있는 개인정보 통합관리 시스템을 신설할 필요가 있다. 우편시스템의 모든 개인정보에 대한 관리 및 보안성 적용 여부를 모니터링하고, 정보보안 이슈 발생 시 이슈의 중요성, 긴급성에 따른 정보전달 프로세스를 마련하며 데이터 생명 주기 관리 통합 및 자동화, 외부기관에 대한 신속한 응대가 가능하도록 전담 업무를 부여하여 권한과 책임을 명확히하고 정보의 신뢰성을 확보할 것이다.

개인정보 통합관리 시스템은 〈표 12〉와 같은 특징을 가지고 구성할 필요가 있다.

〈표 12〉 우편분야 개인정보 통합시스템의 특징

구 분	시스템 특징
개인정보 통합 관리 서비스 지원	○ 내부직원 및 고객의 개인정보 조회, 분석, 삭제 및 일괄암호화가 가능한 관리 화면 신설 ○ 우편시스템 서버 접근 이력정보 기능 강화 및 관리 화면 신설 ○ 개인정보 관리 표준 마련(고객관리시스템의 고객정보, 사용자 신상정보 등) ○ 내부자 보안통제 기능 구현 – 화면, 데이터 접근 권한에 따른 차등적 데이터 접근 기능 개발 마련 및 관리 화면 신설
데이터 생명주기 관리	○ 우편종별 보관기한에 따른 데이터 생명주기 관리 가이드 통합 ○ 데이터 생명 주기에 근거한 자동 삭제 모듈 개발 ○ 데이터 생명 주기 대상 통합 관리(조회, 삭제 등) 화면 신설
정보보안 이슈 전파	○ 정보보안 이슈 전파 프로세스 마련 (예) 긴급공지: 휴대폰 문자서비스 이용 일반공지: 알림 팝업 및 시스템 로그인 시 팝업 생성 최우선 설정

Ⅴ. 맺음말

정보통신기술은 사용자 ID, 이름, 주소, 성향, 신체적 특성 등 개인정보를 공유하기 용이하고, 이에 축적된 개인정보를 열람, 수집 및 저장할 수 있게 끔 발전되어 왔다. 특히 포털, 오픈

마켓, 게임사 등은 콘텐츠를 사용자에게 맞춤 판매하기 위해 개인정보를 성역 없이 수집 및 분석하고 있다. 정보의 정확도에 따라 광고효과의 차이가 발생하기 때문에 수집되는 정보의 민감도 역시 높아지고 있는 실정이다.

시만텍에서 발표한 자료에 의하면 지하경제 서버를 통해 거래되는 아이템의 가격대는 신용카드가 50센트에서 5달러, 은행 계좌 정보는 30달러에서 400달러로 음성적인 거래가 이루어지고 있는 현실을 볼 때 개인정보의 유출 위험은 더욱 높다고 보여진다.

그리고 우리나라에서 2014년 1월에 발생한 신용카드사의 개인정보 유출과 관련해서 집단소송을 제기하지 않은 피해자들에게도 정신적인 위자료를 지급해야 된다는 입장에서 국민은행, 하나로 텔레콤 등은 최소 10만원에서 30만원까지 정신적 고통에 따른 위자료를 지급해야 된다는 법원의 판결이 있었다.

만약 법원에서 신용카드사 개인정보 유출에 대한 위자료를 인정했다고 할 경우 1억 건의 정보유출에 20만 원씩의 위자료를 인정하면 배상액이 20조 원에 달해 기업의 존폐를 결정지을 수 있는 중요한 요소가 될 것이다. 따라서 한국우정도 보다 견고하고 안정적인 개인 정보 관리체계를 구축하는데 많은 노력과 관심이 그 어느 때 보다 필요한 시기라고 생각된다.

참 고 문 헌

김현동 (2014), 「'정보보호 보험'이 해법이다」, thebell.

(사)개인정보보호협회 (2013), 『개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석』.

우정사업본부 (2014), 정보보호 관련 내부자료.

이용수 (2013), 『미래전략 구현을 위한 중장기 IT 전략 로드맵 수립』, 정보통신정책연구원.

최윤형 (2012), 「개인정보보호의 이해 및 안전한 관리」.

한국인터넷진흥원 (2013), 『2012년 개인정보 보호 상담 사례집』.

_____ (2014), 「유럽연합, 개인정보보호 강화를 위한 'EU 개인정보보호 지침' 가

이드라인 발표」.

한은영 (2014), 「일본 개인정보보호법 개정의 배경 및 개정안의 주요 내용」, 『정보통신방송정책 통권 581』, 정보통신정책연구원.

http://privacy.kisa.or.kr/kor/privacy/privacy01_new.jsp

http://isis.kisa.or.kr/sub07/index.jsp?pageId=070500