

공익사항에 관한 감사원 감사청구서(단체용)

수신 : 감사원장

청구일자 : 2015. 03. 19.

1. 청구 단체	단 체 명	경제정의실천시민연합		
	소 재 지	서울 종로구 동숭3길 26-9 경실련회관		
	대 표 자			
	단체설립목적	우리사회의 경제정의와 사회정의를 실현하기 위한 평화적 시민운동을 전개함으로써 민주복지사회의 기틀을 마련하는데 이바지하고자함.		
	허가신고등록기관	기획재정부		
	회 원 의 수	2만3천명	조직년월일	1989. 11. 4
	연락전화 등	전화	02-765-9732	FAX
2.	감사대상기관	행정자치부, 방송통신위원회		
3.	감사청구 제목 : 공공아이핀 부정발급 사고에 대한 관련부처 주의의무위반 등에 대한 감사			
4. 감사 청구 사항	① 공공/민간아이핀 관련부처 주의의무위반 건 - 행정자치부의 공공아이핀 운영의 개인정보보호법 위반 - 행정자치부 공공아이핀시스템 관리 및 운영의 주의의무위반 - 방송통신위원회의 민간아이핀관리 및 운영의 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반 ② 행정자치부 「부정발급」 등의 통지미이행			
5. 청구 이유	별첨.			
6. 관련 증거 자료	증 제1호. 행정자치부 보도자료(2015.03.05.) 증 제2호. 행정자치부 보도자료(2015.03.10.) 증 제3호. 데이터넷 기사(2015.03.06.) 증 제4호. 행정안전부 보도자료(2008.07.16.) 증 제5호. 연합뉴스 기사(2010.06.07.) 증 제6호. 보안뉴스 기사(2010.06.07.) 증 제7호. 머니투데이 기사(2015.03.12.) 증 제8호. 연합뉴스 기사(2015.03.06.) 증 제9호. 머니투데이 기사(2015.03.09.) 증 제10호. 파이낸셜뉴스 기사(2014.01.20.) 증 제11호. JTBC 뉴스기사(2015.03.08.) 증 제12호. 서울신문 기사(2015.03.06.) 증 제13호. 연합뉴스 기사(2015.03.05.)			

I. 감사청구사항

- 행정자치부는 2015. 3. 5. 공공아이핀 약 75만건이 부정발급되는 사고가 발생했다고 발표했습니다. 행정자치부 보도자료에 따르면 2월 28일 00시 30분부터 3월 2일 09시 까지 지역정보개발원에서 관리하고 있는 공공아이핀시스템의 프로그램 취약으로 인해 공공아이핀이 75만 건 부정발급 되었습니다. 이 중 12만건의 게임사이트 등에서 사용된 것도 드러났습니다. (증 제1호 참조)
 - 공공아이핀은 이미 2010년에도 부정발급되어 사회적 문제를 일으켰음에도, 다시 같은 형식의 부정발급사고가 발생되었는바, 이는 공공아이핀을 관련법에 규정된 것과 달리 다목적으로 포괄적으로 사용할 수 있도록 하여 이를 관리하지 않았고, 유출통지 등 기본적인 사고방지조치를 취하지 않은 것이 가장 큰 원인이 되었습니다. 특히 사고를 인지한지 10여일이 지난 지금까지도 부정발급된 정보주체들에게 통지절차들이 이루어 지고 있지 않습니다.
 - 이에 저희 단체는 ▲행정자치부가 공공아이핀을 「개인정보보호법」에서 정한 것과 달리 다목적으로 사용하도록 허용하고 있는 것, ▲공공아이핀 부정발급 사고 대처방안과 시스템 부실 등에 대한 주의의무위반과 「개인정보보호법」에 따른 통지조치를 이행하지 않은 것, ▲민간아이핀을 관리감독하고 있는 방송통신위원회의 주의의무위반과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 정한 것과 달리 다목적으로 사용하도록 허용하고 있는 것에 대한 감사원의 감사와 처리가 필요하다고 판단 되어 아래 사항에 대한 감사를 청구하는 바입니다.
- 1) 공공/민간아이핀 관련부처 주의의무위반 건
 - 행정자치부의 공공아이핀 운영의 개인정보보호법 위반
 - 행정자치부 공공아이핀시스템 관리 및 운영의 주의의무위반
 - 방송통신위원회의 민간아이핀관리 및 운영의 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반
 - 2) 행정자치부 「부정발급」 등의 통지미이행

II. 감사청구이유

1. 공공/민간아이핀 관련부처 주의의무위반건

□ 행정자치부의 공공아이핀 운영의 「개인정보보호법」 위반

- 행정자치부는 공공아이핀의 근거를 「개인정보보호법」 제24조의2 제2항이 정한 대체수단으로 보고 있습니다. 그리고 지금까지 이를 범용으로 사용하도록 허용하고 있습니다.
- 그러나 「개인정보보호법」 제24조의2 제2항은 같은 법 제1항에서 정한 각호의 경우에만 제한적으로 대체수단이 사용가능한 것으로 되어 있어 행정자치부가 이를 범용으로 사용허용한 것은 현행법위반이라 할 것입니다.

□ 행정자치부 공공아이핀시스템 관리 및 운영의 주의의무위반

- 행정자치부의 2015. 3. 10.자 “공공아이핀 부정발급 종합대책 추진” 보도자료에 따르면 이번 사고는 “시스템의 취약점을 이용하여 정상 공공아이핀 발급단계를 우회한 파라미터 위변조 방식이 사용” 되었다고 밝히고 있습니다.(증 제2호 참조) 전문가들은 이러한 ‘파라미터 변조’ 공격은 “매우 초보적인 공격으로 상당히 많은 해킹에 사용되고 있지만, 방어는 까다로운 것으로 알려진다.” 라고 평가하고 있습니다. (증 제3호 참조) 행정자치부는 아래에서 보듯 이러한 간단한 보안조치도 취하지 아니하면서 I-PIN 보급을 확대한 것은 시민들의 안전할 권리를 침해할 수 있는 것이 예견되어 있습니다.
- 행정자치부 전신인 행정안전부는 2008년 7월경 “주민등록번호 보호 종합대책”을 발표하면서 첫 번째 주요 핵심과제로 “온라인상 주민번호 대체수단의 보급을 확대하고, 기능을 개선한다”고 발표하였고, 구체적인 내용으로 I-PIN 보급의 확대를 방법으로 제시하였습니다. (증 제4호 참조) 그러나 I-PIN 보급의 확대와 함께 관련 보안조치들이 적극적으로 제시되지 않았습니다.

- 결국 2010년에 13,000여개의 아이핀이 부정발급 되고 중국의 게임 아이템 판매 조직이나 국내 광고업자 등에게 3,500만원에 팔아넘겨지는 사건이 발생하였습니다. (증 제5호 참조) 이러한 상황이 발생하였음에도 불구하고 정부(방송통신위원회)는 아이핀의 사용범위를 법이 정한 예외적인 경우를 제한하고, 부정발급되는 경우에 이를 통지하고, 근본적으로는 주민등록번호의 사용을 금지하는 등의 대책을 마련하지 아니하고 주먹구구식으로 “아이핀을 더욱 안전한 제도로 발전시켜, 인터넷 상에서 발생하는 주민등록번호의 유출에 따른 문제를 해소할 수 있도록 노력할 것”이라는 발표를 하기도 하였습니다. (증 제6호 참조)
- 행정자치부의 이번 대규모 공공아이핀의 부정발급은 예견된 참사로 간단한 해킹 조차도 대응하지 못한 것이 벌써 수차례 나타난 일입니다. 즉, 이번 공공아이핀 부정발급 사건이 반복해서 발생한 사실을 미루어 보아, 행정자치부가 해킹 등에 대한 대비·예방의 노력에 최선을 다했다고 인정하기 어려울 만큼 허술한 시스템 관리 사실 등이 확인되었다 할 것입니다.

□ 방송통신위원회 민간아이핀 관리 및 운영의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 위반

- 이와 같이 공공아이핀 부정발급 사건이 발생함에 따라 주민등록번호를 근간으로 하는 유사한 시스템인 민간아이핀에 대한 시민들의 우려도 커지고 있습니다. 현재 공공아이핀과 민간아이핀 모두 공공과 민간 영역 구분 없이 동일하게 쓰고 있음에도 각각 관리감독 부처, 발급기관 등이 분산되어 있습니다. (증 제7호 참조)
- 민간 아이핀의 근거는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의2 제2항에서 정한 대체수단으로, 이 법에서 정하는 대체수단은 같은 법 제23조의2 제1항이 정한 각호의 예외사유에만 한정적으로 사용되는 것으로 해석되어야 합니다.
- 그럼에도 불구하고 민간아이핀을 목적제한없이 포괄적으로 사용할 수 있는 것처럼 관리감독하고 있는 방송통신위원회는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 위반의 위법행위를 하고 있다 하겠습니다.
- 더 나아가 방송통신위원회는 공공아이핀 부정발급 사건이 발생하고 나서야 “안

전성 강화를 위해 2차 인증을 의무화하는 방안을 추진할 계획”이라며 대책을 내놓았습니다. 그러나 추후 확인결과 “발급 단계가 한 차례 더 많아지면, 이용자들이 번거로워질 수 있기 때문”에 “아직 고려 중”이라고 설명하였습니다.(증 제8호, 제9호 참조) 즉, 민간아이핀 역시 공공아이핀과 유사하게 주의의무위반에 해당하지 않는지를 검토하여 업무상 주의의무위반에 해당하는지 감사해야 할 필요가 있다 할 것입니다.

- 또한 해당 업무 등과 관련하여, 방송통신위원회가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3에서 정한 본인확인기관 지정 업무에 있어서 심사 등 지정절차를 충실히 이행하고 있는지, 그리고 같은 법 제23조의4에서 정한 본인확인기관에 대한 업무 정지 및 지정취소 등의 의무 및 역할을 충실히 이행하고 있는지에 대해서도 검토해야 할 필요가 있습니다. 지난 2014년 1월, 3개 신용카드사 개인 정보 유출사건이 본인확인기관인 코리아크레딧뷰로(KCB) 직원에 의해 유출되는 등 본인확인기관의 개인정보 유출 사건이 반복적으로 발생함에도 불구하고, 이들 기관이 본인확인업무를 계속하고 있는 점 등을 미루어보아 해당 사안에 관해서도 반드시 감사를 실시해야 할 필요가 있다 할 것입니다.(증 제10호 참조)

□ 소 결

- 위에 제시한 사안 등을 미루어 보아, 공공아이핀 부정발급 사건에 있어서 행정자치부가 수행해야 할 주의의무를 충실히 이행하였다고 볼 수 없습니다. 또한 사건이 발생한 후에야 대책을 모색하고 점검에 착수한 방송통신위원회 역시 해당 직무를 충실히 이행하였다고 볼 수 없습니다.

2. 행정자치부의 부정발급 등의 통지미이행

□ 「개인정보보호법」 제34조 제1항 위반

- 행정자치부는 지난 3월 5일 해당 사건 관련 leaked 발표에 대해 “보고받고 나서 2차 피해, 부정발급된 아이핀을 어디에다 쓰고 어떤 용도에 쓰고 요런 것 파악해서 조치하는데 집중” 하였다고 설명하였습니다.(증 제11호 참조)

- 하지만 해당 사건으로 인해 개인정보가 유출 된 피해자(정보주체)들에게는 ▲유출된 개인정보의 항목, ▲유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 등 「개인정보보호법」 제34조 제1항에서 규정하고 있는 개인정보 유출통지 의무를 이행하지 않았습니다.
- 현재까지도 행정자치부는 해당 사건이 유출된 주민번호가 이용됐는지 조차 명확하게 파악하지 못하고 있습니다. 다만 공공아이핀 발급에 이름과 주민번호가 필수이고, 부정 발급된 공공아이핀과 동일한 개인정보로 가입된 이용자가 게임사이트 3곳에 8천명이나 있었던 점으로 미뤄 공격주체가 미리 확보한 개인정보를 이용해 시스템 공격에 이용했을 것으로 추정됩니다.(증 제12호 참조)
- 이러한 사실관계에 미루어보아 75만건의 공공아이핀 부정발급이 이루어지면서 공격주체가 이용한 (유출된) 개인정보가 공공아이핀 발급을 위해 지역정보개발원 등에 축적되어 있던 개인정보와 매칭되며 유출되었을 것을 알 수 있습니다.
- 하지만 행정자치부는 부정 발급된 아이핀으로 개인정보가 유출됐는지 등을 인지하지도 못하고 있음은 물론, 관련법에서 규정하고 있는 유출통지마저 충실히 이행하지 않아 이미 발생하였거나 발생할 수도 있는 피해를 방지하는 행태를 보였습니다.(증 제13호 참조)

□ 소 결

- 「개인정보보호법」에서는 개인정보 피해자들에게 유출통지 등을 이행하지 않을 경우 5천만원 이하의 과태료를 부과하고 있습니다. 그만큼 개인정보 유출사건이 발생했을 시 해당 사실을 피해자(정보주체)들에게 신속하게 알려 피해를 최소화하기 위해 노력을 기울여야 합니다.
- 행정자치부는 개인정보보호법에서 규정하고 있는 통지의무를 다하지 않았는바, 감사원의 공정한 감사를 통하여 개인정보 유출통지 등이 신속하게 이루어져야 할 것입니다.

Ⅲ. 결론

- 공공아이핀 부정발급 사건은 우리나라 전반에 걸친 개인정보 유출사건 등의 심각성을 여실히 보여주는 사건에 해당합니다. 본인확인 등을 위해 무분별하게 수집한 시민들의 개인정보를 정부부처마저 보호를 위해 제 의무를 다하지 않는 모습을 보여주었습니다.
- 시민들은 이러한 정부부처의 행태에 공분하고 있으며, 개인정보 유출사건이 재발하지 않도록 철저한 조사와 이에 따른 처벌, 나아가 개인정보 보호를 위한 근본대책이 마련되기를 바라고 있습니다.
- 하지만 주무부처인 행정자치부가 개인정보 보호를 위해 면피적 행태를 보여주고, 심지어 소관 법령에서 규정하고 있는 기본적인 피해구제 절차조차 이행하지 않아 시민들의 불신을 증폭시켰습니다. 이로 인해 사건이 알려진 지난 3월 5일과 6일 이틀 동안 1,065명에 달하는 시민들이 공공아이핀 서비스를 탈퇴하였습니다.(증 제11호 참조)
- 대규모 개인정보 유출사건이 계속되어 시민들은 극도의 불안감을 느끼고 있습니다. 2014년에도 카드사, 이동통신사 등에서 대규모 개인정보 유출사건이 발생하였고 수많은 대책들이 쏟아져 나왔지만, 개인정보 유출사건을 막지 못하고 있습니다.
- 특히 이번 사건의 경우 “개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적”으로 하는 「개인정보보호법」을 주관하고 있는 행정자치부가 당사자에 해당하기 때문에 더욱 더 명백한 사실관계 규명과 그에 따른 엄정한 조사 및 처벌이 반드시 뒤따라야 합니다.
- 위에서 명시한 것과 같이 행정자치부는 시민들의 개인정보 보호를 위해 사전적 예방노력은 물론 사후적으로도 시민들의 피해구제 등을 위해 최선을 다한 것으로 볼 수 없습니다. 심지어 「개인정보보호법」에서 규정하고 있는 개인정보 유출통지 등과 같은 기본적인 조치조차 취하지 않았습니다. 이는 행정자치부의 명백한 직무유기이자 관련법 위반사안에 해당합니다.

- 이에 공공아이핀 부정발급 사건에 있어 행정자치부의 직무 등에 대해 명확한 조사를 통해 행정 운영의 개선과 향상을 기함은 물론 시민들의 개인정보 보호를 위한 신속한 조치가 이루어질 수 있도록, 감사원은 행정자치부의 사무와 직무 등에 대해 철저한 감사를 실시해 줄 것을 당부합니다.

2015. 3. 19.

경제정의실천시민연합

감 사 원 귀중