개인정보보호법 위반 행정처분 결과 분석 및 이용자 권리보장을 위한 제안

전주현*, 노시완*, 이경현**
*부경대학교 일반대학원 정보보호학과
**부경대학교 컴퓨터공학부
jhjeon@pukyong.ac.kr, nosiwan@pukyong.ac.kr, khrhee@pknu.ac.kr

An Analysis of the Publication of Administrative Penalties for Violation of the Personal Information Protection Act

Ju-Hyun Jeon*, Siwan Noh*, Kyung-Hyune Rhee**,
*Department of Information Security, Graduate School,
Pukyong National University
**Division of Computer Engineering, Pukyong National University

요 약

개인정보 보호법 위반 시 법률적 기준에 따라 행정처분을 하고 이에 대한 결과를 공표하게 된다. 개인정보보호위원회가 심의·의결 기관에서 국무총리 산하 중앙행정기관으로 출범하고 난 이후 개인정보보호법 위반으로 인한 행정처분 결과 공표 자료를 분석하였다. 공표 대상이 되는 주요 산업군과 위반 법률 조문을 분석해 향후 정보주체 권리 보장을 위한 안전한 보호 방안을 제안한다.

1. 서론

개인정보보호위원회는 기존 심의·의결 기관에서 2020년 8월 데이터 3법 개정 이후 국무총리 산하 중앙행정기관으로 출범하였다. 때문에, 기존에는 행정안전부가 공공기관 및 오프라인 사업자, 방송통신위원회는 온라인 사업자, 신용정보를 다루는 금융회사는 금융위원회가 행정 관리를 하였으나 이를 일괄 통합함으로써 개인정보에 대한 컨트롤타워 마련 등 개인정보 분야에 있어 큰 변화가 생겼다. 하지만 금융분야 신용정보에 대한 부분은 여전히 금융위원회가 관리하고 있어 개인정보 보호법은 일반법의 성격을, 신용정보법은 특별법의 성격을 지니게 되었다. 법률 또한 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에서 개인정보에 대한 부분이 '개인정보보호법' 특례 조항으로 통합되었다[1]. 개인정보보호위원회가 중앙행정 기관으로 출범한 이후 개인정보보호법은 '보호' 위주의 기존 규제에서 '활용'도 가능한 법 개정이 되었기 때문에 위반에 따른 행정처분 결과 공표 자료는 중요한 가치를 지닌다[2]. 본 논문은 어떤 산업과 어떤 법률 조항을 주로 위반하였는지를 분석해 정보주체 권리 보장을 위한 안전한 조치 강화 방안을 제시하는데 본 의의가 있다.

2. 관련연구

행정안전부에서는 개인정보보호법 위반 시 행정처분을 공표하는 공표제도를 두고 있다. 개인정보보호법 위반 행정처분 결과에 대한 법적 근거는 개인정보보호법 제66조 및 동법 시행령 제61조에 따라 개선명령, 시정조치, 과태료 부과의 내용 및 결과를 공표할 수 있다고 명시한다. 공표기준은 기존 ① 위반사유 및 피해 범위 (중과실, 대규모, 사회적 물의) ② 위반 기간 및 횟수 (2년 이상, 3년 내 동일 위반 2회 이상) ③ 개선 노력 (개선의지, 조치결과 미제출) 3개 항목 중에서 2개 동시에 해당하는 경우 공표하였다. 2014년 8월 개선된 공표기준을 적용해 현재까지 기준으로 삼아 공표하고 있으며 표 1의 공표기준 7개 항목 중 어느 1개라도 해당하는 경우 개인정보보호위원회 홈페이지를 통해 공표된다.

<표 1> 개인정보 위반시 행정처분 공표기준

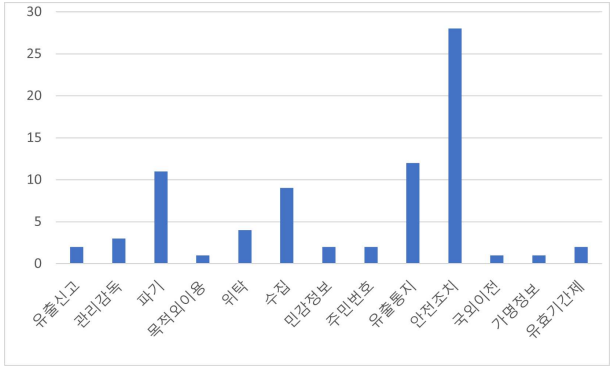
① 위반내용: 은폐·조작행위 ② 위반정도: 과태료 부과금액 1천만원 이상 ③ 위반기간: 6개월 이상 지속 ④ 위반횟수: 최근 3년 내 2회 이상 위반 ⑤ 피해범위 : 피해자 수 10만명 이상 ⑥ 피해결과: 2차 피해 발생 등 ⑦ 검사 거부·방해, 시정조치 미이행

특히, 개인정보보호법 위반으로 인한 공표에는 기관이나 기업이 실명으로 공개되기 때문에 부정적인 이미지와 신뢰에 큰 영향을 미치게 된다. 공표제도를 개선 강화한 이유도 민감정보나 주민등록번호 유출 등 중요한 개인정보 유출에 대한 경각심을 가지게 하기 위한 개인정보보호에 대한 정부의 의지가 반영되었다. 개인정보 보호법 위반 행정처분 결과 공표 제도는 2011년 도입된 제도로서, 시행 이후, 공표 기준이 너무 엄격하게 설정돼 있어 실효성이 없다는 지적이 있었는데, 2014년 1월에 발생한 카드사 개인정보 유출사고를 계기로 2014년 8월에 공개를 확대하는 방향으로 공표기준을 개선하였으며, 2015년 8월에 처음으로 1개 업체를 실명으로 공표한 바 있다[3].

3. 분석 및 평가

개인정보보호위원회 홈페이지에 공개된 개인정보보호법 위반에 따른 행정처분 공표 자료를 수집하고 공표건수 18건, 처분건수 78건, 처분대상 35곳을 분석하였다[4]. 공표한 시기는 개인정보보호위원회가 출범하고 난 이후 2021년 1월에서 동년 12월까지 공표 자료를 기준으로 하였다. 공표 시 데이터3법 개정 이전 정보통신망법을 적용한 공표 대상 10곳도 포함되었다. 개인정보보호법과 정보통신망법 조문별 분류보다는 개인정보 라이프사이클(Life-cycle)의 처리단계별 의무위반 사항과 고유식별정보, 민감정보, 국외이전 등 개인정보 주요 이슈로 분류하였다.

(단위:건)



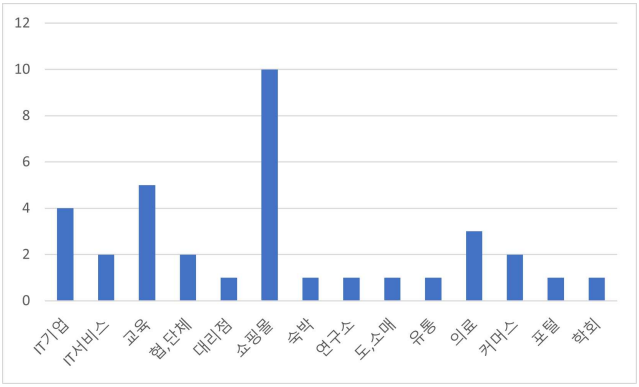
(그림 1) 개인정보 행정처분 결과 공표 분석

3.1 처리단계별 위반사항 및 주요 조문별 분류

개인정보 수집(9건), 위탁(4건), 목적 외 이용(1건), 파기(11건), 관리감독(3건), 민감정보(2건), 주민번호(2건), 국외이전(1건), 가명정보(1건), 유효기간제(2건), 유출신고(2건), 유출통지(12건), 안전조치(28건) 등으로 분석되었다(그림 1). 행정처분 결과에 따른 공표된 자료를 분석해 보면 수집, 위탁, 파기, 유출통지, 안전조치 위반 형태가 다수 반복적으로 이루어졌다. 안전조치에 대한 위반 건수가 다른 조문에 비해 높은 개인정보보호법 제29조 안전조치의무가 하위 고시에 관리적·기술적·물리적 조치로 세부적 요구사항을 명시하고 있기 때문이다. 고시 위반은 개인정보보호법 제29조 법률 위반으로 연결되기 때문에 위반 사항을 분석해 보면 항상 안전조치의무 위반이 일반적으로 많이 나타나는 것으로 분석된다[2].

3.2 산업별 유형별 분류

공표된 자료를 산업 분야별로 분석한 결과는 (그림 2)와 같다. 세부적으로 살펴보면 일반적인 IT기업(4건), IT서비스(2건), 교육(5건), 협,단체(2건), 대리점(1건), 쇼핑몰(10건), 숙박(1건), 연구소(1건), 도,소매(1건), 유통(1건), 의료(3건), 커머스(2건), 포털(1건), 학회(1건)으로 분석되었다. 정보통신서비스제공자의 대표적인 쇼핑몰이 가장 많았으며 교육분야, 의료분야, IT기업, 커머스 형태로 분류되었다. 온라인을 통한 개인정보처리가 많기 때문에 정보통신서비스제공자가 더 강화된 의무조치가 요구된다. 교육과 의료분야에도 유출로 이어지면 더 큰 피해가 생겨 집중적으로 개인정보를 보호해야 하는 분야이다.



(그림 2) 개인정보 행정처분 공표 산업별 분석

3.3 행정처분 내용에 따른 분류

개인정보보호법 위반으로 행정처분으로 과태료, 과징금, 시정권고·명령, 공표 등으로 행정처분이 내려진다. 개선권고는 법률 위반은 아니며 주된 행정처분은 과태료 처분으로 이루어진다. 최근 들어 페이스북, 넷플릭스, 구글 등 해외 글로벌기업에도 과징금 부과 사례가 증가하고 있다[5].

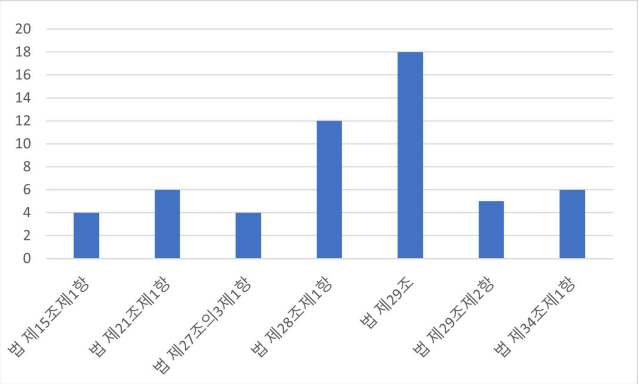
본 논문에서 분석한 자료를 바탕으로 행정처분을 분석하면 표 2와 같다. 행정처분으로는 시정명령과 과태료 처분이 대부분을 차지하고 있고 시정명령과 과태료 부과가 동시에 처분되는 경우가 많았다. 과태료 처분 금액도 최소 100만 원에서부터 최대 2,600만 원까지 부과된 것으로 분석되었다.

<표 2> 행정처분 결과 분석

행정처분	과태료	과징금	시정명령	개선권고
	76건	0건	44건	2건

3.4 법률 위반 조문별 유형 분석

가장 많은 위반을 한 법률 조문 위주로 분석한 결과 정보통신망법 포함하여 법 제29조(18건), 법 제28조제1항(12건), 법 제34조제1항(6건), 법 제21조제1항(6건), 법 제29조제2항(5건), 법 제15조제1항, 법 제27조의3제1항이 각각 4건으로 분석되었다(그림 3).



(그림 3) 법 조문별 위반 건수 분석 결과

3.5 공공기관 행정처분 과태료 처분 사례

개인정보보호위원회는 '공공기관 개인정보 처리실태 점검 계획('21.1.13)'을 수립하고, 개인정보 보호법 위반 소지가 있는 20개 공공기관을 선정하여 조사를 진행한 뒤, 19개 기관의 법규 위반사항을 확인했다. 점검 결과 5개 지방자치단체(교육청 2개 포함)에 개인정보 법규 위반에 따른 과태료를 부과하였는데 이는 개인정보 보호법 제정(2011년 3월) 이후 첫 사례이다[6].

개인정보보호법 대상으로 적용되는 대표적인 곳이 공공기관이다. 개인정보보호법 제정 전에 '공공기관 개인정보보호에 관한 법률'에 공공기관은 분리되어 적용되었으나 개인정보보호법 제정 이후 기존 법률은 폐지 되면서 개인정보보호법에 공공기관과 민간이 통합 적용되는 일반법적 성격을 가지게 되었다. 개인정보보호위원회가 중앙행정기관으로 출범하면서 공공기관을 실태점검을 통해 지자체 및 교육청 그리고 대학교 등 공공기관에도 과태료를 부과하기 시작하였다. 위반내용을 살펴보면 대부분 법 제29조에 따른 안전조치의무 위반이다(표 3).

<표 3> 공공기관 행정처분 사례

기관분류	처분 건수	과태료	위반내용
지자체(3)	7건	1,920만 원	안전조치
교육청(2)	4건	960만 원	안전조치
대학교(9)	18건	4,140만 원	안전조치
그 외(5)	10건	2,340만 원	안전조치

행정처분은 ①개선권고 ② 시정명령 ③ 과태료부과 ④ 공표 순으로 진행된다. 행정처분 결과에서 공표기준 7가지에 부합되면 실명으로 공표되기 때문에 기관 경영평가에도 영향을 미친다. 개인정보처리자 중에 하나인 공공기관이 개인정보보호법 위반 및 유출사고 사전예방 및 정보주체 권리 보장에 의무가 더 요구된다.

4. 정보주체와 이용자 권리보장을 위한 제안

이 장에서는 정보주체와 이용자 권리보장을 위한 다음의 3가지 사항을 제안한다.

- **기술적 보호 유형별 평가지표 개발:** 개인정보보호법 제29조 안전조치의무 위반이 다수 공표됨에 따라 개인정보처리자 및 정보통신서비스제공자 등에 기술적 보호조치에 대한 관리·감독을 강화해야한다. 권한부여, 접근통제, 접속기록, 암호화, 보안프로그램 설치 등에 대한 기술적 보호 조치 평가지표 개발한다.
- **취약한 산업분야 행정, 기술, 재정지원:** 정부에서는 자율규제를 통한 협,단체 지원을 강화하고 취약한 산업분야에 대해 실태점검이나 기획점검을 실시해 개인정보보호에 대한 법률적 위반사항을 지도·점검 해야한다. 취약한 산업분야는 자율적 규제를 활성화하여 협,단체에서 가이드하는 실천수칙을 강화함에 따라 개인정보보호 취약 산업분야에서 유출사고로 이어지는 위험을 감소시킬 수 있다.
- **경제적 제재로 처벌 전환 :** 공공과 민간 모두 형사처벌의 제재 보다는 경제적 제재 처벌 수위가 강화됨에 따라 실질적인 의무조치 사항이 반영 되도록 유도하는 것이 바람직하다. 이는 경제

적 제재가 강화되면 의사결정자의 법 준수성 유무에 따른 비용증대나 절감효과를 바로 체감 가능하기 때문에 보다 효율적인 제재 수단이된다. 유럽의 GDPR이나 미국의 CCPA 같은 법률에서 법의 강제성이 실효성 있는 이유는 거액의 벌금에 대한 처벌 때문인 경우가 많다.

5. 결론 및 향후연구

본 논문에서는 데이터3법 개정 이후 출범한 개인정보보호위원회가 형사처벌이 아닌 행정처벌 결과 공표한 자료를 분석해 법률 위반 유형과 산업분야, 위반 법 조문별 유형, 그리고 최근 공공기관 과태료 부과를 분석하고 기술적 보호조치 유형별 지표개발, 취약한 산업분야에 대한 실태점검 강화, 경제적 처벌 강화 등의 정보주체 및 이용자 권장보장에 따른 제도적 실행을 제안하였다. 개인정보보호법을 위반하게 되면 여러 가지 경로로 형사처벌 및 행정처분을 받게된다. 일반적으로 개인정보처리자 및 정보통신서비스제공자 등이 개인정보 유출 사고로 인해 자체적으로 인지하지 못한 상황에서 해킹, 내부통제 미흡으로 발생한 경우가 많았고 유출신고, 유출통지 등에 대한 과태료부과가 다수 있어 유출사고가 생기면 신고와 통지는 법률적 절차에 따라 신속하게 실행하여야 한다. 공표된 자료를 분석한 결과로 수집, 위탁, 목적 외 이용, 파기 개인정보 처리단계별 의무조치 사항에서 위반사항이 있었다. 개인정보를 보관하거나 이용하기 위한 기술적 조치인 법 제29조 안전조치의무 위반이 다수 행정처벌로 과태료가 부과되었고 이는 하위 고시 기준에 명시된 권한부여, 접근통제, 암호화, 접속기록, 보안프로그램 설치등 세부적인 조치 항목이 다수 있기에 많은 부분 위반하여 행정처분 받은 것으로 분석되었다. 또한, 이미 유출사고가 발생하고 나서 유출통지 및 유출신고 지연에 따른 과태료부과 행정처분을 받은 곳도 많았다. 향후에는 개인정보보호위원회가 출범 후 공표한 자료 부족으로 분석의 한계가 있었으며 출범 전 공표한 자료를 추가로 분석하면 더 신뢰성 있는 분석이 될 것이다. 안전성확보조치 기준 고시와 기술적 관리적보호조치 기준 고시에 명시된 세부적인 유형으로 분류해 분석한다면 안전조치의무 위반에 많은 도움이 될 것이다. 개인정보 행정처분 내용 및 결과 공표제도는 가장 보수적인 기준에서 위반사항을 공개하는 것이니만큼 개인정보처리자 및 정보통신서비스제공자 등에 보호조치 의무 위반에 경각심을 주는데 본 논문이 기여할 것으로 기대한다.

사사표기

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었으며 (IITP-2022-2020-0-01797) 일부는 2022년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2021R1I1A3046590).

참고문헌

[1] 강신욱, 데이터 3법 개정의 주요 내용과 관련 쟁점에 대한 소고, BFL(서울대학교 금융법센터), 102권0호, p.53-67, 2020.07

[2] 김세영, 김인석, AHP 기법을 이용한 금융회사『개인정보의 안전성 확보조치 기준』우선순위에 관한 연구, 한국전자거래학회지 제24권 제4호, p.31-47, 2019.11

[3] 행정자치부, 「개인정보보호법」위반업체 실명공개, 보도자료, 2016.2.2

[4] 개인정보보호위원회 www.pipc.go.kr

[5] 개인정보보호위원회, 개인정보위, 개인정보보호 법규 위반 해외기업에 과징금, 보도자료, 2021.8.25

[6] 개인정보보호위원회, 개인정보보호 법규 위반, 지자체도 제재처분의 예외일 수 없다, 보도자료, 2021.09.08