개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2023-006-048호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2023. 4. 12.

주 문

1. 피심인에 대하여 다음과 같이 시정을 명한다.

가. 피심인은 수탁자가 개인정보를 안전하게 처리하는지 처리현황 점검 등 감독하여야 한다.

나. 피심인은 재발방지를 위한 개인정보 처리 절차와 수단을 마련하고, 개인정보보호책임자와 개인정보취급자를 대상으로 정기적인 개인정보 보호교육을 실시하여야 한다.

다. 피심인은 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 6,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보보호법」(이하 '보호법'이라 한다.) 제2조제6호나목에 따른 공공기관으로 보호법 제2조제5항에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	직원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 유출신고((1차) '21.1.30, (2차)'21.2.16)에 대하여 개인정보 관리실태 현장조사('21.3.29.~3.30. 4.12, 4.20)를 통해 피심인의 개인정보 보호법규 위반행위와 관련하여 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 '홈페이지'를 운영하면서 '21. 4. 20. 기준 64,072건의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	수집·이용 항목	수집일	건수(명)
회원정보		'19.7월 ~ 현재	64,072
시험 접수 정보		'19.10월 ~ 현재	54,381

나. 개인정보 유출 경위

□ 피심인은 한국인터넷진흥원(KISA) 개인정보탐지조사팀으로부터 모니터링 중 노출 탐지 사실을 통보받아 2회에 걸쳐 유출신고하였다.

1 1차 유출신고('21.1.30) : '19~'20년도 시험 접수자 정보 관련

1) 유출경위

피심인의 홈페이지 특정경로에 접근통제가 적용되어 있지 않아 비인가자의 접근이 허용되어 구글 검색엔진에서 개인정보가 유출되었다.

2) 유출경과 및 대응

- ('21. 1. 29.) 한국인터넷진흥원(KISA) 탐지조사팀의 유선 연락을 받고 로그 분석을 통해 외부자가 조회한 것을 확인하여 개인정보 유출인지
- ('21. 1. 30.) 피심인 홈페이지에 개인정보 유출사실 공지, 개인정보보호 포털에 개인정보 유출 신고, 정보주체에게 유출 사실 통지(문자전송)

3) 유출규모 및 항목

'19~'20년도 접수자 49,694명의 개인정보(이름, 아이디, 전화번호(휴대폰), 생년월일, 학교, 학년)

② 2차 유출신고('21.2.16) : '12~'14년도 시험응시료 환불 정보 관련

1) 유출경위

피심인이 '15년에 "시험응시료 환불정보" 조회 제공을 위해 홈페이지에 명단을 팝업으로 올리고 환불 완료 이후 삭제하지 않아 빙(bing.com) 검색엔진에서 개인정보 유출*되었다.

2) 유출경과 및 대응

- ('21. 2. 15.) 한국인터넷진흥원(KISA) 탐지조사팀의 메일 수신 후 로그 분석을 실시하여 외부자가 조회한 것을 확인하여 개인정보 유출 인지
- ('21. 2. 16.) 피심인 홈페이지에 개인정보 유출사실 공지, 개인정보보호 포털에 개인정보 유출 신고, 정보주체에게 유출 사실 통지(문자전송)

3) 유출규모 및 항목

'책과함께' 사업제휴사인 교원구몬의 '12~'14년도 시험 응시료 환불 4,324건의 개인정보(이름, 계좌번호, 학부모 연락처(휴대폰), 지국명)

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 2. 27. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 3. 17.

위반 사실을 인정하고 위반사항에 대해 전부 시정을 완료하였다는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법 규정

가. 보호법 제21조제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.”라고 규정하고 있다.

나. 보호법 제26조제4항은 “위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.”라고 규정하고 있다.

다. 보호법 제29조는 “개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제30조제1항은 안전성 확보조치로 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(2호), 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(3호), 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조 · 변조 방지를 위한 조치(4호)를 하도록 하고 있다.

같은 법 시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준」(이하 '고시'라고 한다.)에서는 "개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다.(제6조제3항)", "개인정보처리자는 비밀번호 및 생체인식정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.(제7조제2항)", "개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다.(제8조제1항)", "개인정보처리자는 개인정보의 오ㆍ남용, 분실ㆍ도난ㆍ유출ㆍ위조ㆍ변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다.(제8조제2항)", 라고 규정하고 있다.

2. 위법성 판단

가. 개인정보의 파기를 소홀히 한 행위

피심인은 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 하나, 홈페이지에서 회원탈퇴를 한 223명의 개인정보를 파기하지 않고 보관한 행위는 보호법 제21조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	세부내용(고시 등)
개인정보의 파기 미흡	보호법 §21①	개인정보가 불필요하게 되었을 때 지체없이 파기하지 않은 행위

나. 업무위탁에 따른 관리·감독을 소홀히 한 행위

피심인은 제3자에게 개인정보의 처리 업무를 위탁하는 경우에 위탁자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 하나, 홈페이지 수탁사인 ㈜○○○, ㈜○○○○에 대한 처리현황 점검 등 관리·감독을 하지 않은 행위는 보호법 제26조제4항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
수탁사 관리감독 소홀	보호법 §26④	§28⑥	수탁사를 교육하고 처리 현황 점검 등 관리·감독하지 않은 행위

다. 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ①취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 하며, ②비밀번호 및 바이오정보는 암호화하여 저장하여야 하고 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 하며, ③개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 하며, ④개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 하나, ①홈페이지 로그인 없이 구글 검색엔진에서 개인정보가 조회되도록 한 사실, ②홈페이지에서 개인정보취급자 및 정보주체의 비밀번호를 'SHA1'으로 양방향 암호화하여 저장한 사실, ③홈페이지의 접속기록 중 '처리한 정보주체 정보, 수행업무

(수정·삭제·다운로드)’를 보관·관리하지 않는 사실, ④접속기록에 대한 점검을 하지 않은 사실은 보호법 제29조를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보 보호조치 위반 (접근통제, 암호화, 접속기록)	보호법 §29	§30①	· 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§6③) · 비밀번호를 저장하는 경우 일방향 암호화로 저장하지 않은 행위(고시§7②) · 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하지 않은 행위(고시§8①) · 개인정보처리시스템의 접속기록 등을 월 1회이상 점검하지 않은 행위(고시§8②)

Ⅳ. 처분 및 결정

1. 시정조치 명령

피심인의 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)제4항을 위반한 행위에 대하여 제64조제1항에 따라 다음과 같이 시정을 명한다.

가. 피심인은 수탁자가 개인정보를 안전하게 처리하는지 처리현황 점검 등 감독하여야 한다.

나. 피심인은 재발방지를 위한 개인정보 처리 절차를 마련하고, 개인정보 보호책임자와 개인정보취급자를 대상으로 정기적인 개인정보 보호교육을 실시하여야 한다.

다. 피심인은 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 과태료 부과

피심인의 보호법 제21조제1항(개인정보의 파기), 제29조(안전조치의무) 위반에 대한 과태료는 같은 법 제75조(과태료)제2항제4호 및 제2항제6호, 같은 법 시행령 제63조의 [별표2]「과태료 부과기준」에 따라 다음과 같이 부과한다.

가. 기준금액

보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 제21조(개인정보의 파기) 제1항, 제29조(안전조치의무) 위반에 대해서 각 1회 위반에 해당하는 과태료인 600만 원을 적용한다.

< 과태료 부과기준, 개인정보보호법 시행령 제63조 [별표 2] >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
마. 법 제21조제1항·제39조의6(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제4호	600	1,200	2,400
자. 법 제23조제2항, 제24조제3항, 제28조제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

「개인정보보호법 위반에 대한 과태료 부과기준」('과태료 부과지침') 제8조(과태료의 가중)는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(조사방해, 위반의 정도, 위반기간, 기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 보호법 제29조(안전조치의무) 위반행위는 과태료 부과지침 제8조의 과태료 가중기준에 따라 위반행위별 각 목의 세부기준에서 정한 행위가 3개인 점을 고려하여 기준금액의 10%인 60만원을 가중한다.

< 과태료의 가중기준(제8조 관련) >

기준	가중사유	가중비율
위반의 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우	기준금액의 50% 이내
	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내

※ 과태료 부과지침 제8조에 따라 과태료의 가중은 기준금액의 50%를 초과할 수 없음

다. 과태료의 감경

과태료 부과지침 제7조(과태료의 감경)는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(당사자 환경, 위반정도, 조사협조 및 자진시정 등, 개인정보보호 노력정도, 사업규모, 기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 경우, 사전통지 및 의견제출 기간이 종료되기 이전에 위반상태를 모두 시정을 완료한 점, 조사 기간 중 행위사실을 인정하면서 자료제출·진술 등 조사에 적극 협력한 점 등을 종합적으로 고려하여 과태료 부과지침 제7조의 과태료 감경기준에 따라 기준금액의 50%를 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사 협조·자진 시정 등	1. 과태료의 사전 통지 및 의견 제출 기간 내에 법규 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50% 이내
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 40% 이내

라. 최종 과태료

피심인의 개인정보 보호법 제21조제1항 및 제29조를 위반한 행위에 대하여 기준금액에서 가중·감경을 거쳐 총 660만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제21조(개인정보의 파기)제1항	법 제75조제2항제4호	600	-	300	**300**
제29조(안전성확보 조치 의무 위반)	법 제75조제2항제6호	600	60	300	**360**
계		1,200	60	600	**660**

3. 결과 공표

「개인정보 보호법」제66조제1항 및 「개인정보보호위원회 처분 결과 공표기준」(2020.11.18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 법 제75조제2항 각호에 해당하는 위반행위를 2개 이상 한 경우(제4호)에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표 개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		법 제21조	개인정보의 파기	2023. 4. 12	과태료 300만 원
		법 26조	업무위탁에 따른 개인정보의 처리제한		시정 명령
		법 제29조	안전조치의무 위반 (접근통제, 암호화, 접속기록)		과태료 360만 원
2023년 4월 12일 개 인 정 보 보 호 위 원 회					

V. 결론

피심인의 보호법 제21조제1항, 제26조제4항 및 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등)제1항, 제75조(과태료)제2항제4호 및 제2항제6호, 제66조(결과의 공표)제1항에 따라 시정명령, 과태료 부과, 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날로부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2023년 4월 12일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　강 정 화　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　백 대 용　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　염 흥 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)