개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2024-007-176호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2024. 4. 24.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 5,400,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 개선을 권고한다.

   가. 피심인은 참여 들이 가명정보 처리 관련 기록을 작성·보관 하도록 지도·감독한다.

   나. 피심인은 가명정보 처리시 「가명정보 처리 가이드라인」에 따른 가명처리 단계별 절차[1](사전준비→위험성 검토→가명처리→적정성 검토→안전한 관리 등 5단계)를 준수하는 등 가명정보에 대한 안전성 확보 조치*를 이행하도록 지도·감독한다.

* (예시) 가명정보 처리기록 작성·보관, 원본정보와 분리 보관, 가명정보 안전조치 및 재식별 금지, 내부관리계획 수립, '가명처리 단계별 절차' 이행, 가명정보의 처리에 관한 사항을 처리 방침에 공개 등

다. 피심인은 시스템에 대한 접근권한 부여 현황을 재검토하여, 관리자 페이지에 접근할 수 있는 '참여 소속 '와 각각의 들이 보유한 접근권한을 필요최소한으로 조정한다.

라. 피심인은 참여 소속 개인정보취급자에 대해 가명정보 처리 관련 교육을 실시한다.

마. 피심인은 가.부터 라.의 개선권고에 따른 조치를 이행하고, 통지를 받은 날로부터 60일 이내에 개인정보 보호위원회에 이행 결과를 제출한다.

이 유

Ⅰ. 기초 사실

피심인은 「舊 개인정보 보호법」(법률 제16930호, 이하 "舊 보호법") 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

피심인명	사업자등록번호	대표자 성명	주소	직원 수

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보정책국이 **국민신문고 민원**[*]('23. . .)을 처리하면서 피심인의 **舊 보호법 위반 혐의에 대해 조사를 요청**('23. . .)함에 따라, 조사조정국

1) 가명정보 처리 가이드라인('24.2월) 10~38쪽

에서 조사를 실시('23. 7. 14. ~ 10. 16.)한 결과, 피심인의 舊 보호법 위반행위와 관련된 다음과 같은 사실을 확인하였다.

* 이 수집.생성하는 정보(회원정보 및 정보 등)가 개인정보 또는 가명정보에 해당하는지와 안전성 확보조치 필요 여부를 질의

2. 개인정보 수집·이용 현황

피심인은 빅데이터 분석을 통한 등을 위해 시스템*(이하 ' ')을 운영하면서 회원정보 및 정보를 처리 하고 있다.

* '14. 1월에 오픈하였으며, 현장점검일 기준 전국 개가 참여 중

개인정보파일 (개인정보처리시스템)	수집항목	수집일	수집목적	수집방법	보유기간	건수(명)

3. 사실조사 결과

가. 시스템 운영 관련 기초 사실

○ 피심인은 「 빅데이터 사업」에 참여하는 들로부터 회원정보와 정보를 제공받아 추천 서비스 등에 이용하였다.

- '14. 1월, ' 빅데이터 분석·활용 사업'을 개시, '14~'23년 기간 중 해당 사업에 참여할 공모*

* 매년 4월경 지자체, 교육청 소속 및 등을 대상으로 해당 사업에 참여할 신규 공모(참여 시 운영평가 10점 가점)

- **'14년 시스템을 구축**하고 참여 의 DB에서 **회원정보 및 정보를 매일 1회 업데이트**(야간)

○ 참여 들은 회원 **원본정보를 토대**로 **특정 개인이 식별되지 않는 정보만 추출된** 회원정보 및 정보를 피심인에 제공하였다.

- **(회원정보)** 의 지침에 따라 사용자key*, 우편번호(세부주소 없음), 생년(월일은 1월 1일로 고정), 성별 등 11개 항목으로 구성된 **별도의 View Table을 생성하여 해당 정보만 제공**

* 사용자key는 각 회원가입 순서대로 부여된 연번을 기반으로 생성되어, 동일인이라도 마다 각기 다른 연번값을 가지며, 일방향 암호화(SHA256 등)함

(그림 삭제)

< 회원 정보의 원본 데이터와 수집 데이터 간 비교 >

컬럼명	회원정보 Table	View Table(제공) ⇨	수집 Table
사용자Key *자동생성번호	12345	3132333435	5cb403a99a1b72ec43…
가족아이디	abc123	5343332313	feec2273d9894b701a7…
이름	홍길동	X(미제공)	X(미수집)
생년월일	2000-05-30	2000-01-01 *월일은 1.1일로 고정	2000-01-01
주소	헬리오시티 203동 101호	X(미제공)	X(미수집)
우편번호	05698	05698	05698
성별	2	2	2
회원가입일	2010-05-01	2010-05-01	2010-05-01
정보수정일	2015-05-30	2015-05-30	2015-05-30
회원등급(기호)	0	0	0
제적일자	2020-05-30	2020-05-30	2020-05-30
탈퇴일자	2020-05-30	2020-05-30	2020-05-30

- **(정보)** 방식, 일시 등 회원별 행태 정보

<피심인이 각 으로부터 제공 받는 정보>

구 분	회원정보 수집 항목	데이터 수집항목
원본 제공항목	생년, 우편번호(집), 성별, 회원가입일, 가입 코드, 등록일시, 탈퇴일시	
(암호화 대상)	사용자key, 가족아이디key	사용자key

나. 보호법 적용 법리 : 가명정보 여부 및 당사자 적격 판단

○ **(가명정보 여부)** 참여 이 피심인의 지침에 따라 생성하는 회원 정보는 **원본정보로부터 특정 개인을 알아볼 수 없도록 가공한** 것으로서 **보호법 제2조 제1호 다목에 따른 가명정보에 해당하며,**

※ 피심인은 점검일 기준 '통계작성'을 목적으로 '가명처리'를 하고 있다고 소명

> * **(보호법 제2조 제1호 다목) 가명정보**는 개인정보의 일부를 삭제하거나 전부를 대체하는 등의 방법으로 추가정보 없이는 특정 개인을 알아볼 수 없도록 처리함으로써 **원래 상태로 복원하기 위한 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보**

- 사용자Key 등이 일방향 암호화(SHA256 등) 되었더라도, **원본 DB와 결합 되면 특정 개인을 알아볼 수 있는 정보**로서 안전조치 의무 등 **가명정보 처리 특례**(보호법 §28의2 ~ §28의5)가 적용된다.

○ **(당사자 적격) 피심인과 참여 모두** 가명정보 처리에 관여하므로 **보호법상 의무를 준수할 책임**이 있다.

- **(참여)** 보유한 회원 개인정보를 **가명 처리한 주체**이며, 에 **가명정보를 제공한 자**에 해당한다.
- **(피심인)** 참여 으로부터 **가명정보를 제공받은 자**에 해당한다.
- **(양자 간의 관계)** 각 은 법령에 따라 상호 협력체계로 운영, **피심인을 정점으로 업무상 지휘체계**를 갖추고 있어, 이 사건 시스템도 시행령 제 조제 호에 따른 **협력망의 일종**으로 **소속을 달리하는 참여(공모) 및 정보의 제공 관계**로 볼 수 있다.

> **(관련법령 삭제)**

다. 가명정보 처리 특례 위반 관련 기초사실

○ **(접근통제)** 피심인은 개인정보 취급자인 소속 직원이 관리자 페이지에 인터넷망을 통해 접속할 때, **아이디와 비밀번호만으로 로그인이 가능**하도록 운영한 사실이 있다.

○ **(접속기록)** 피심인은 관리자와 소속 직원들이 관리자페이지 및 DB에 **접속한 기록을 일부 누락**하여 보관·관리한 사실이 있다.

- 관리자페이지 로그인 기록에 아이디, 아이피, 접속일시를 기록하고 있으나, 수행업무 및 처리주체 정보를 누락 하였고, DB 접속기록은 보관·관리하지 않았다.

○ **(대장관리)** 피심인은 참여 으로부터 **제공받은 가명정보 처리 관련 기록을 작성·보관하지 않은 사실**이 있다.

라. 참여 의 보호법 위반 가능성 등에 대한 조치 검토

○ 참여 도 **가명정보 생성·제공 과정에서 관련 기록을 작성·보관하지 않았을 가능성***이 높으나, 아래와 같은 사유로 **피심인의 지도를 통한 개선**이 효과적이라고 판단하였다.

* 참여 들은 가명정보 개념이 도입('20. 8. 5일 시행된 보호법에 처음 규정) 되기 훨씬 전인 **'14년부터 가명 처리**를 하였고, **지침을 시달한 피심인 조차 관리대장을 작성하지 않은 점**으로 미루어 볼 때, 상당수가 **위반 가능성** 있음

- ①피심인 조사 과정에서 법 위반 가능성이 추정될 뿐 참여 전체(여 개)에 대한 **사실조사가 이루어지지는 못한 점**, ②**피심인의 지휘체계 아래** 「 빅데이터 사업」에 참여하게 된 점(참여 시 평가점수 10점/ 점 가점) 등을 고려할 때, ③ 법에 따라 **피심인의 지도를 통해 행정 목적 달성이 가능한 점**을 종합 고려하였다.

Ⅲ. 위법성 판단

1. 가명정보에 대한 안전성 확보 조치를 소홀히 한 행위

가. 관련 법 규정

舊 보호법 제28조의4제1항은 “개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

또한, 舊 시행령 제29조의5제1항은 “개인정보처리자는 법 제28조의4제1항에 따라 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보에 대하여 제30조 또는 제48조의2에 따른 안전성 확보 조치(1호)를 해야 한다.“라고 규정하고 있다.

나. 위법성 판단

개인정보처리자가 가명정보를 처리하는 경우에는 舊 시행령 제30조에 따른 안전성 확보 조치를 하여야 하나, 참여 담당자가 인터넷망을 통해 관리자페이지에 접속하고 있음에도, 피심인이 **아이디와 비밀번호만으로 관리자 페이지에 로그인이 가능하도록 운영한 것**은 **舊 보호법 제28조의4제1항, 舊 시행령 제29조의5제1항제1호 및 舊 고시*** **제6조제2항 위반으로 판단된다.**

* 개인정보의 안전성 확보 조치 기준(2020.8.11., 개인정보위 고시 제2020-2호)

2. 가명정보 처리관련 기록을 작성·보관하지 않은 행위

가. 관련 법 규정

舊 보호법 제28조의4제2항은 “개인정보처리자는 가명정보를 처리하고자

하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.”라고 규정하고 있다.

또한, 舊 시행령 제29조의5제2항은 “법 제28조의4제2항에서 “대통령령으로 정하는 사항”이란 가명정보 처리의 목적(1호), 가명처리한 개인정보의 항목(2호), 가명정보의 이용내역(3호), 제3자 제공 시 제공받는 자(4호), 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항(5호)을 말한다.“라고 규정하고 있다.

나. 위법성 판단

개인정보처리자가 가명정보를 처리하는 경우에는 관련 기록을 작성하여 보관하여야 하나, 피심인이 **이를 작성하여 보관하지 않은 행위는 舊 보호법 제28조의4제2항, 舊 시행령 제29조의5제2항 위반에 해당한다.**

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’23. 11. 1. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ‘24. 1. 24. 개인정보보호위원회에 법 위반사실을 인정하고 시정을 완료하였다는 의견을 제출하였다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제28조의4제1항 및 제2항 위반행위에 대해 같은 법 제75조제4항제6호와 제6의2호, 舊 시행령 제63조의 [별표2]에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊 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 舊 보호법 제28조의4 제1항 및 제2항 위반행위에 대해 **1회 위반에 해당하는 과태료인 600만 원과 200만 원을 각각 적용**한다.

< 舊 보호법 시행령 제63조 [별표 2] - 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
머. 법 제28조의4제2항을 위반하여 관련 기록을 작성하여 보관하지 않은 경우	법 제75조 제4항제6의2호	200	400	800

나. 과태료의 가중

「舊 개인정보보호법 위반에 대한 과태료 부과기준」(개인정보위 2023. 3. 8. 이하 '舊 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.

같은 조 제1항 위반행위에 대하여 위반행위별 각 목의 세부기준에서 정한 행위가 2개인 점과 법 위반상태의 기간이 3개월 이상인 점을 고려하여 **기준금액(600만 원)의 20%인 120만 원을 가중**한다.

피심인의 舊 보호법 제28조의4제2항 위반행위에 대하여 법 위반상태의 기간이 3개월 이상인 점을 고려하여 **기준금액(200만 원)의 10%인 20만 원을 가중**하고,

< 舊 과태료 부과지침 [별표 2] - 과태료 가중기준 >

기준	가중사유	가중비율	
위반의 정도	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내	합계 상한 50% 이내
위반 기간	법 위반상태의 기간이 3개월 이상인 경우	기준금액의 50% 이내	

다. 과태료의 감경

舊 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 노력 정도, ▲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.

피심인은 조사 기간 중 일관되게 행위 사실을 인정하면서 자료 제출 등 조사에 적극 협력하였고, 위반행위를 시정 완료하였으므로, 舊 과태료 부과지침 제7조 [별표1] 감경기준에 따라 **기준금액(총 800만원)의 50%인 400만 원을 감경**한다.

< 과태료 부과지침 [별표 1] - 과태료 감경기준 >

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

라. 최종 과태료

피심인의 舊 보호법 제28조의4 제1항 및 제2항 위반행위에 대하여 **기준금액(총 800만 원)에서 가중·감경을 거쳐 총 540만 원의 과태료를 부과**한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만 원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제28조의4 제1항	법 제75조제2항제6호	600	120	300	**420**
제28조의4 제2항	법 제75조제4항제6의2호	200	20	100	**120**
합계		800	140	400	**540**

2. 개선권고

피심인 주도로 진행되는 협력망 운용 관련 사안이므로 피심인에 대하여 법 제61조제2항에 따라 다음과 같이 개선을 권고한다.

가. 피심인은 참여 들이 가명정보 처리 관련 기록을 작성·보관하도록 지도·감독한다.

나. 피심인은 가명정보 처리시 「가명정보 처리 가이드라인」에 따른 가명처리 단계별 절차[2](사전준비 → 위험성 검토 → 가명처리 → 적정성 검토 → 안전한 관리 등 5단계)를 준수하는 등 가명정보에 대한 안전성 확보 조치*를 이행하도록 지도·감독한다.

* (예시) 가명정보 처리기록 작성·보관, 원본정보와 분리 보관, 가명정보 안전조치 및 재식별 금지, 내부관리계획 수립, '가명처리 단계별 절차' 이행, 가명정보의 처리에 관한 사항을 처리 방침에 공개 등

다. 피심인은 시스템에 대한 접근권한 부여 현황을 재검토하여, 관리자페이지에 접근할 수 있는 '참여 소속 '와 각각의 들이 보유한 접근권한을 필요최소한으로 조정한다.

라. 피심인은 참여 소속 개인정보취급자에 대해 가명정보 처리 관련 교육을 실시한다.

마. 피심인은 가.부터 라.의 개선권고에 따른 조치를 이행하고, 통지를 받은 날로부터 60일 이내에 개인정보 보호위원회에 이행 결과를 제출한다.

2) 가명정보 처리 가이드라인('24.2월) 10~38쪽