개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2024-217-572호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인

의결연월일 2024. 8. 28.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 7,800,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대한 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간 공표한다.

이 유

Ⅰ. 기초 사실

야구 홈페이지( )를 운영하는 피심인은 「舊 개인정보 보호법」[1](이하 '舊 보호법')에 따른 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수(명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 포털(privacy.go.kr)에 유출 신고('22. 3. 29.)한 피심인에 대하여 개인정보 취급·운영 실태 및 舊 보호법 위반 여부를 조사('22. 10. 5. ~ '23. 6. 30.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 야구 홈페이지( )를 운영하면서, '22. 10. 28. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

1) 법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행

< 개인정보 수집 현황 >

구분	항목	수집일	건수
합 계			1,837

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지 및 대응 내용
‘22. 3. 29.	11:35	한국인터넷진흥원으로부터 야구 홈페이지 개인정보 유출 정황에 대한 안내메일 접수
	-	개발업체에서 해킹 사실을 확인하며 개인정보 유출인지
	-	이용자 대상 개인정보 유출통지(홈페이지)
	17:43	개인정보 포털을 통한 개인정보 유출신고
‘22. 3. 30. ~	-	웹서버 내 악성코드 등 의심파일 삭제, 개인정보 파기 및 홈페이지 폐쇄*

* 현재 피심인은 개인정보를 처리하지 않는 홈페이지( )를 재구축하여 공개·운영중

2) 유출항목 및 규모

이용자 명의 이름, 휴대전화번호, 이메일이 유출되었다.

3) 유출 경위

신원 미상의 자(이하 ‘해커’)가 웹셸* 공격으로 피심인이 운영하는 웹사이트에 침입하여 개인정보를 유출한 것으로 추정되며,

* 웹셸(Webshell) : 업로드 취약점을 통하여 시스템에 명령을 내릴 수 있는 코드, 웹셸 설치 시 보안 시스템을 피하여 별도의 인증 없이 시스템에 쉽게 접속 가능

해커가 실행한 것으로 추정되는 웹셸 파일기록 등은 남겨져 있으나 접속기록

등이 보존·관리되지 않아 자세한 유출경위·시기는 파악이 불가하였다. 다만, 서비스를 ’14. 7. 21. 종료하였음에도 불구하고, DB 테이블 내 최신 데이터 등록 시점이 ’20. 7. 27. 로 확인되어 ‘20. 7. 27. 직후에 유출된 것으로 추정된다.

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 파일 업로드 취약점 등 홈페이지 취약점에 대한 점검 및 조치를 적절하게 수행하지 않아 웹셸이 업로드되어 실행되었고, 그 결과 피심인이 보유중인 개인정보가 유출되었다. 또한, 개인정보에 대한 접속기록을 보관하고 정기적으로 확인·감독하지 않아 불법 접근 및 개인정보 유출을 인지하지 못하는 등 안전조치 의무를 소홀히 하여 개인정보가 유출된 사실이 있다.

나. 불필요해진 이용자의 개인정보를 파기하지 않은 행위

피심인은 서비스를 위해 ’11. 7. 22. ~ ’14. 7. 21. 기간 동안 이용자의 개인정보 1,837건을 수집·이용하였으나, 서비스가 종료(‘14. 7. 21.)된 후 개인정보 처리목적이 달성되어 불필요해진 개인정보를 파기하지 않고 보관한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’23. 7. 4. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’23. 7. 21. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 舊 보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·

변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령[2](이하 ‘舊 시행령’) 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

舊 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

舊 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 舊 개인정보의 기술적·관리적 보호조치 기준[3](이하 ‘舊 기술적 보호조치 기준’) 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있으며,

제5조제1항은 “정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.”라고 규정하고 있다.

나. 舊 보호법 제21조제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.”고 규정하고 있다.

2. 위법성 판단

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2020. 10. 20. 시행
3) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15., 시행

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 ’20. 7. 27. ~ ’22. 3. 30. 동안 웹셸이 업로드되고 실행되는 것을 방지하기 위해 파일 업로드 취약점 등 홈페이지 취약점 점검과 조치를 적절히 수행하지 않고 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항제2호, 舊 기술적 보호조치 기준 제4조제9항을 위반한 것이다.

또한, 피심인이 개인정보처리시스템에 대한 접속기록을 보존·관리하지 않은 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항제3호, 舊 기술적 보호조치 기준 제5조제1항을 위반한 것이다.

나. 불필요해진 이용자의 개인정보를 파기하지 않은 행위

[舊 보호법 제21조제1항(개인정보의 파기)]

피심인이 서비스 종료로 처리목적이 달성되어 불필요해진 ’11. 7. 22. ~ ’14. 7. 21. 기간 수집한 회원정보 1,837건에 대해 ’22. 3. 30. 까지 파기하지 않고 보관한 행위는 舊 보호법 제21조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	舊 보호법 §29	舊 시행령 §48의2① 제2호	・열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위 (舊 기술적 보호조치 기준 §4⑨)
		舊 시행령 §48의2① 제3호	・개인정보처리시스템에 접속한 기록을 최소 1년 이상 접속기록을 보존·관리하지 않은 행위 (舊 기술적 보호조치 기준 §5①)
개인정보 파기 위반	舊 보호법 §21①	舊 시행령 §16	・처리목적 달성 등 개인정보가 불필요하게 되었음에도 지체없이 파기하지 않은 행위

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무), 舊 제21조(개인정보의 파기) 위반행위에 대한 과태료는 같은 법 제75조제2항제4호·제6호, 舊 시행령 제63조, 舊 시행령 [별표2] '과태료의 부과기준' 및 '舊 개인정보 보호법 위반에 대한 과태료 부과기준[4]'(이하 '舊 과태료 부과지침')에 따라 다음과 같이 부과한다.

가. 기준금액

舊 시행령 제63조와 [별표2] '과태료의 부과기준'은 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위의 기준금액을 600만 원으로 산정한다.

< 舊 시행령 [별표2] 과태료의 부과기준 중 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 **제29조**를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	舊 보호법 제75조 제2항제6호	600	1,200	2,400
마. 법 **제21조제1항**·제39조의6을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	舊 보호법 제75조 제2항제4호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

舊 과태료 부과지침 제8조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여, 舊 과태료 부과지침의 '[별표2] 과태료의 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.

4) 개인정보보호위원회지침, 2023. 3. 8. 시행

피심인의 舊 보호법 제29조(안전조치의무) 위반행위는 ‘법 위반상태의 기간이 3개월 이상인 경우’, ‘제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우’에 해당하여 10%씩 가중한 기준금액의 20%를 가중하며,

舊 보호법 제21조제1항(개인정보의 파기) 위반행위는 ‘법 위반상태의 기간이 3개월 이상인 경우’에 해당하여 기준금액의 10%를 가중한다.

2) 과태료의 감경

舊 과태료 부과지침 제7조는 ‘사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여, 舊 과태료 부과지침의 ’[별표1] 과태료의 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 舊 보호법 제29조(안전조치의무) 위반행위 및 舊 보호법 제21조제1항(개인정보의 파기) 위반행위의 경우 ‘시정을 완료한 경우(50% 이내)’, ‘조사에 적극 협력한 경우(40% 이내)’에 해당하여 최대 감경 범위인 기준금액의 50%를 각각 감경한다.

다. 최종 과태료

피심인의 舊 보호법 제21조제1항(개인정보의 파기), 제29조(안전조치의무) 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 780만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제, 접속기록)	600만원	120만원	300만원	**420만원**
개인정보의 파기 의무	600만원	60만원	300만원	**360만원**
계				**780만원**

2. 결과 공표

舊 보호법 제66조제1항 및 '舊 개인정보 보호위원회 처분결과 공표기준[5]」제2조(공표요건)에 따라, 피심인의 위반행위는 법 제75조제2항 각호에 해당하는 위반행위를 2개 이상 한 경우(제4호), 위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)에 해당하므로, 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침[6]」에 따라 공표 기간은 1년으로 한다.

<table>
<tr><td colspan="6">개인정보보호법 위반 행정처분 결과 공표
개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.</td></tr>
<tr><td rowspan="2">순번</td><td rowspan="2">위반행위를 한 자</td><td colspan="2">위반행위의 내용</td><td colspan="2">행정처분의 내용 및 결과</td></tr>
<tr><td>명칭</td><td>위반조항</td><td>위반내용</td><td>처분일자</td><td>처분내용</td></tr>
<tr><td rowspan="2">1</td><td rowspan="2"></td><td>舊 보호법* 제21조제1항</td><td>개인정보의 파기 의무</td><td rowspan="2">2024. 8. 28.</td><td>과태료 360만 원</td></tr>
<tr><td>舊 보호법 제29조</td><td>안전조치의무 (접근통제, 접속기록)</td><td>과태료 420만 원</td></tr>
<tr><td colspan="6">* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2024년 8월 28일
개 인 정 보 보 호 위 원 회</td></tr>
</table>

Ⅴ. 결론

피심인의 舊 보호법 제21조제1항(개인정보의 파기), 제29조(안전조치의무) 위반행위에 대해 같은 법 제75조(과태료)제2항제4호·제6호, 제66조(결과의 공표)제1항에 따라 과태료 부과, 결과 공표를 주문과 같이 의결한다.

5) 개인정보보호위원회지침, 2020. 11. 18. 시행
6) 개인정보보호위원회지침, 2023. 10. 11. 시행

이의제기 방법 및 기간

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(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2024년 8월 28일

위 원 장 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)