개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2025-002-005호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 ㈜동행복권 (사업자등록번호 :)

대표자

의결연월일 2025. 1. 22.

주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

   가. 과 징 금 : 503,000,000원

   나. 과 태 료 : 4,800,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인은 처분등에 대한 통지를 받은 날부터 1개월 이내 당해 처분등을 받은 사실 등을 피심인의 홈페이지 및 모바일 어플리케이션에 2일 이상 게시하여야 한다. 이때, 구체적인 공표내용과 방법 등은 개인정보보호위원회와 미리 문서로 협의를 거쳐야 한다.

이 유

Ⅰ. 기초 사실

피심인은 복권 발행·관리 및 판매, 복권시스템 구축·운영 등 업무와 이와 관련된 개인정보 처리 업무를 복권위원회로부터 위탁받아 처리하는 자로서 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 복권 판매사이트를 운영하면서, 신원 미상의 자(이하 '해커')로부터 다수 계정의 비밀번호가 무단으로 변경되어 이용자의 개인정보가 유출되었음을 확인하고 신고('23. 11. 6.)하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 11. 17. ~ '24. 5. 22.) 하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 '23. 11. 24.(자료제출일) 기준 건의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구 분	항 목	기 간	건 수(건)
계			

나. 개인정보 유출 관련 사실관계

피심인은 '19. 10. 16. 회원 본인인증 방식 개선 과정에서 취약점*이 존재하는 '비밀번호 찾기 페이지' 소스코드를 등록·배포하였다.

* '비밀번호 찾기 페이지'에서 ID 입력 및 별도 인증(이메일 등) 이후 비밀번호 변경이 진행되나, 이때 인증받은 ID가 아닌 다른 ID로 입력을 조작하면 바꾼 ID의 비밀번호가 변경됨

해커는 '23. 11. 4. '회원가입 페이지'에서 ID 중복 체크 기능을 활용하여 사전에 비밀번호 변경 대상(ID) 목록을 확보하였고,

* 48개 IP에서 계정 중복 여부를 확인하는 패킷이 대량(1,800만여회)으로 발생

'23. 11. 5. '비밀번호 찾기 페이지'의 취약점을 활용하여 입력 ID를 바꿔가며 임의로 비밀번호를 변경 및 로그인하여 회원정보 페이지에 접속 후 개인정보를 열람하였다.

1) (유출 규모 및 항목) 회원 749,114명의 개인정보*

* 이름, 생년월일, 전화번호, 이메일, 아이디, 계좌번호, 주소

2) 유출 인지 및 대응

일 시	유출인지 및 대응 내용
’23.11.5. 11:58	고객센터 접수민원을 통해 침해사고 **최초인지**
‘23.11.5. 17:45	해킹 침해사고 홈페이지 공지
‘23.11.5. 18:59	복권 포털사이트 임시 폐쇄
’23.11.5. 19:22	개인정보 **유출 신고**(KISA)
‘23.11.6. 11:04	개인정보 **유출 신고**(사이버수사대)
‘23.11.6. 11:58	개인정보 **유출 대상자에게 통지**(문자)
‘23.11.6. 15:30	개인정보 **유출 대상자에게 통지**(이메일)

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

피심인은 ’19. 10. 16. 회원 본인인증 방식 개선 과정에서 비밀번호 변경을 요청한 회원과 실제 비밀번호 변경 대상을 확인하지 않는 취약점이 존재하는 소스코드를 등록·배포한 사실이 있다.

피심인은 보안장비(Anti-DDoS, IPS, 웹방화벽 등)를 구축·운용하였으나, 네트워크 응용계층(L7)에서 대량 접속 시도를 탐지할 수 있는 정책을 운영하지 않아 사전에 공격 시도를 충분히 의심할 수 있는 과도한 접속 시도가 있었음에도 불구하고, 이를 탐지·차단하지 못한 사실이 있다.

※ ‘23. 11. 4. 1개 IP에서 최대 808,676회 이상, 52개 IP에서 각 100회 이상 회원 ID 조회,
’23. 11. 5. 1개 IP에서 최대 757,183회 이상, 32개 IP에서 각 50회 이상 비밀번호 변경

피심인은 분리보관하고 있는 일부 휴면회원의 계좌번호를 ‘19. 12. 6. 이후 암호화하지 않은 상태로 관리한 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 ‘24. 10. 23. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 11. 6. 개인정보보호

위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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[1](이하 ‘시행령’) 제30조제1항제2호는 “개인정보에 대한 접근 권한을 제한하기 위해 ‘개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 대한 기준의 수립·시행(가목)’, ‘정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한 인증수단 적용 기준의 설정 및 운영(나목)’, ‘그 밖에 개인정보에 대한 접근 권한을 제한하기 위하여 필요한 조치(다목)’를 하여야 한다.”라고 규정하고 있고, 제3호는 “개인정보에 대한 접근을 통제하기 위해 ‘개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치(가목)’, ‘개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단(나목)’, ‘그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)’를 하여야 한다.”라고 규정하고 있고, 제8호는 “그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.”라고 규정하고 있다. 또한, 제4호는 “개인정보를 안전하게 저장·전송하는데 암호화 또는 이에 상응하는 조치를 하여야 한다”라고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 개인정보의 안전성 확보조치 기준[2](이하 ‘안전성 확보조치 기준’) 제6조1항은 “정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인

1) 개인정보 보호법 시행령(대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행)
2) 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 시행)

정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도를 탐지 및 대응(제2호)'하는 등의 안전조치를 하여야"하고, 제6조제3항은 "개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다."라고 규정하고 있다. 또한, 제7조제2항은 "계좌번호(제2호) 등 이용자의 개인정보에 대해서는 안전한 알고리즘으로 암호화하여 저장하여야 한다."라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

[보호법 제29조(안전조치의무)]

피심인이 '비밀번호 변경'과 같이 민감한 데이터에 접근하는 기능을 구현하면서 비밀번호 변경 요청자와 변경 대상자가 일치하는지 확인하지 않아 취약점이 발생하도록 하는 등 적절한 점검없이 소스코드를 도입·배포한 행위는 보호법 제29조, 시행령 제30조제1항제2호, 안전성 확보조치 기준 제6조제3항을 위반한 것이다.

피심인이 보안장비를 운영하고 있었으나, 탐지·차단 정책 관리 및 이상행위 대응에 소홀하여 사전에 공격 시도를 충분히 의심할 수 있는 과도한 접속 시도가 있었음에도 불구하고, 이를 확인하지 못하는 등 안전조치를 다하지 않은 행위는 보호법 제29조, 시행령 제30조제1항제3호, 안전성 확보조치 기준 제6조제1항을 위반한 것이다.

피심인이 분리 보관하고 있는 일부 휴면회원의 계좌번호를 암호화하지 않은 행위는 보호법 제29조, 시행령 제30조제1항제4호, 안전성 확보조치 기준 제7조제2항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령(고시)	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§30① 2호 (§6③)	・개인정보가 인터넷 홈페이지 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않고 운영한 행위(고시§6③)
		§30① 3호 (§6①)	・개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도 탐지·차단하지 못한 행위(고시§6①)
		§30① 4호 (§7②)	・계좌번호 등 이용자의 개인정보에 대해서 암호화하지 않고 저장한 행위(고시§7②)

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제29조(안전조치의무), 시행령 제30조제1항제2호·제3호, 안전성 확보조치 기준 제6조제3항·제1항 위반행위에 대해 같은 법 제64조의2제1항제9호, 시행령 제60조의2 [별표 1의5] 및「개인정보보호 법규 위반에 대한 과징금 부과기준[3]」(이하 '과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제64조의2제1항, 시행령 제60조의2에 따라 위반행위가 있었던 사업연도 직전 3개 사업연도의 연평균 매출액의 100분의 3을 초과하지 아니하는 범위에서 부과할 수 있다.

나. 기준금액

1) 중대성의 판단

과징금 부과기준 제8조제1항은 '시행령 [별표 1의5] 2. 가. 1) 및 2)에 따른 위반

3) 개인정보보호 법규 위반에 대한 과징금 부과기준(개인정보보호위원회 고시 제2023-3호, 2023. 9. 15. 시행)

행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준을 기준으로 정한다.’라고 규정하고 있다.

[별표] 위반행위의 중대성 판단기준에 따르면 ‘위반행위의 중대성의 정도는 고려사항별 부과기준을 종합적으로 고려하여 판단’하고, ‘고려사항별 부과수준 중 두 가지 이상에 해당하는 경우에는 높은 부과수준을 적용한다.’라고 규정하고 있으며, ‘고려사항별 부과수준의 판단기준은 ▲(고의 · 과실) 위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려, ▲(위반행위의 방법) 안전성 확보 조치 이행 노력 여부, 개인정보 보호책임자 등 개인정보 보호 조직, 위반행위가 내부에서 조직적으로 이루어졌는지 여부, 사업주, 대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 개인정보의 유출등과 안전성 확보 조치 위반행위와의 관련성을 포함하여 판단, ▲(위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향) 피해 개인정보의 규모, 위반기간, 정보주체의 권리 · 이익이나 사생활 등에 미치는 영향 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 유출등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.’라고 규정하고 있다.

피심인의 고의·과실, 위반행위의 방법, 처리하는 개인정보의 유형, 정보주체의 피해 규모 및 정보주체에게 미치는 영향 등을 종합적으로 고려하여, 위반행위의 중대성을 ’중대한 위반행위‘로 판단한다.

2) 기준금액 산출

과징금 부과기준 제6조제1항은 ‘기준금액은 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액에 부과기준율을 곱한 금액으로 정한다’라고 규정하고 있다.

피심인의 경우, 과징금 부과기준 제7조제3항에 따라 위반행위와 관련이 없는 매출액은 복권 판매와 관련 없는 매출액으로 하고, 직전 3개 사업년도의 연평균 전체 매출액에서 관련 없는 매출액을 제외한 백만원에 시행령 [별표 1의5] 2.

가. 1)에 따른 ‘중대한 위반행위’의 부과기준율 1천분의 15를 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 백만원)

구 분	2020년	2021년	2022년	평 균
①전체 매출액				
②관련 없는 매출액				
①에서 ②를 제외한 매출액				

※ 피심인이 제출한 회계자료를 토대로 작성

<시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	2.1% 이상 2.7% 이하
중대한 위반행위	1.5% 이상 2.1% 미만
보통 위반행위	0.9% 이상 1.5% 미만
약한 위반행위	0.03% 이상 0.9% 미만

다. 1차 조정

과징금 부과기준 제9조에 따라 피심인 위반행위의 기간이 2년을 초과(’19. 10. 16. ~ ’23. 11. 6.)하여 ‘장기 위반행위’에 해당하므로 기준금액의 100분의 50에 해당하는 금액인 천 원을 가산하고,

위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우에 해당하여 기준금액의 100분의 30에 해당하는 금액인 천 원을 감경한다.

라. 2차 조정

과징금 부과기준 제10조에 따라 피심인이 ▲자진 시정 및 조사에 적극 협력한

경우에 해당하여 1차 조정을 거친 금액의 100분의 30에 해당하는 금액을, ▲개인정보 보호 인증(ISMS-P, ISO 27001)을 받은 경우에 해당하여 1차 조정을 거친 금액의 100분의 50에 해당하는 금액을 감경한다. 다만, 1차 조정의 거친 금액의 100분의 50을 초과할 수 없어 천 원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제64조의2제1항제9호, 시행령 제60조의2, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 만 원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
•직전 3개 사업연도 연평균 매출액 (천 원) •연평균 매출액에 1.5% 적용 (중대한 위반)	•위반기간 2년 초과 50% 가중 (천 원) •취득이익 없으므로 30% 감경 (천 원)	•시정완료, 개인정보 보호 인증(ISMS-P) 등을 종합적으로 고려하여 50% 감경 (천 원)	**천 원**

2. 과태료 부과

피심인의 제29조(안전조치의무), 시행령 제30조제1항, 안전성 확보조치 기준 제7조제2항 위반행위에 대한 과태료는 같은 법 제75조(과태료) 제2항제5호, 시행령 제63조[별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[4](이하 '과태료 부과기준')에 따라 다음과 같이 부과한다.

가. 기준금액

시행령 제63조 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라

4) 개인정보 보호법 위반에 대한 과태료 부과기준(개인정보보호위원회 지침, 2023. 9. 15. 시행)

기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 제29조(안전조치의무), 시행령 제30조제1항제4호, 안전성 확보조치 기준 제7조제2항에 대해서는 1회 위반에 해당하는 과태료인 600만 원을 기준금액으로 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		1회	2회	3회 이상
아. 법 **제29조**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제5호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) (과태료의 가중) 과태료 부과기준 제7조는 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표3]의 가중기준에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 보호법 제29조 위반행위(일부 휴면회원의 계좌번호 암호화 미조치)에 대하여 ▲위반기간 2년 초과에 해당하여 과태료 부과기준 제7조에 따라 기준금액의 30%를 가중한다.

2) (과태료의 감경) 과태료 부과기준 제6조는 '당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 보호법 제29조 위반행위(일부 휴면회원의 계좌번호 암호화 미조치)에 대하여 ▲보호법 제32조의2에 따른 개인정보 보호 인증(ISMS-P)을 받은 경우, ▲개인정보 보호 관련 국제인증(ISO27701)을 받은 경우, ▲과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 시정을 완료한 경우, ▲일관되게 행위 사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출 또는 진술하는 등 조사에

적극적으로 협력한 경우에 해당하여 과태료 부과기준 제7조에 따라 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 480만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
암호화 미조치	600만 원	180만 원	300만 원	**480만 원**
계				**480만 원**

3. 처분 결과 공표명령

보호법 제66조제2항 및 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」[5] (이하 '공표 및 공표명령 지침') 제6조제1항에 따라 피심인의 위반행위는 위반상태가 3년을 초과하여 지속된 경우(제7호), 위반행위로 인하여 피해를 입은 정보주체의 수가 10만명 이상인 경우(제8호)에 해당하고, 위반행위가 인터넷을 통하여 이루어졌으므로 제8조 및 제11조에 따라 처분등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분등을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 6분의1 크기로 2일 이상 5일 미만의 기간 동안(휴업일 포함) 공표하도록 명한다. 다만, '1일간 다시 보지 않기' 기능의 사용 등 팝업창 설정방식 등은 보호위원회와 협의하여 정한다.

이때 제7조제1항, 제8조제3항에 따라 원칙적으로 공표지침 [별표]의 표준 공표 문안을 따르되, 공표 문안 등에 관하여 보호위원회와 미리 문서로 협의해야 하고, 제11조제3항에 따라 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 보호위원회와 협의하여 정한다.

5) 개인정보 보호법 위반에 대한 공표 및 공표명령 지침(개인정보보호위원회 지침, 2023. 10. 11. 시행)

Ⅴ. 결론

피심인이 보호법 제29조(안전조치의무)를 위반한 행위에 대하여 같은 법 제64조의2(과징금의 부과)제1항제9호, 제75조(과태료)제2항제5호, 제66조(결과의 공표)제2항에 따라 과징금 부과, 과태료 부과, 공표명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과징금 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 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(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.

2025년 1월 22일

위 원 장 고 학 수 (서 명)

부위원장 최 장 혁 (서 명)

위 원 김 일 환 (서 명)

위 원 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 이 문 한 (서 명)