개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2024-002-008호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 한국고용정보원 (사업자등록번호 : 107-82-11255)
충청북도 음성군 맹동면 태정로 6
대표자 김영중

의결연월일 2024. 1. 24.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 8,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 개선을 권고한다.

가. 피심인은 시스템의 특성을 감안하여 각종 불법적인 접근 시도 가능성에 대비할 수 있도록 임계치 분석·조정 등 시스템 보안 정책 전반을 정비한다.

나. 피심인은 연계 서버를 포함한 시스템 전반의 주민등록번호 보관 상황을 점검하고, 주민등록번호를 암호화하여 안전하게 보관한다.

다. 피심인은 가.부터 나.까지의 개선권고에 따른 조치를 이행하고, 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

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

이 유

Ⅰ. 기초 사실

피심인은 「舊 개인정보 보호법」(이하 '舊보호법'이라 한다) 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	직원 수
한국고용정보원	107-82-11255	김 영 중	충청북도 음성군 맹동면 태정로 6	419명

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 유출 신고('23. 7. 6.)에 따라 피심인의 개인정보 관리실태를 조사('23. 7. 10. ~ 9. 26.)하였으며, 피심인의 舊 보호법 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 구직·구인정보와 직업·진로 정보를 제공하는 고용노동서비스 워크넷(www.work.go.kr)을 운영하면서 아래와 같이 개인정보를 처리하고 있다.

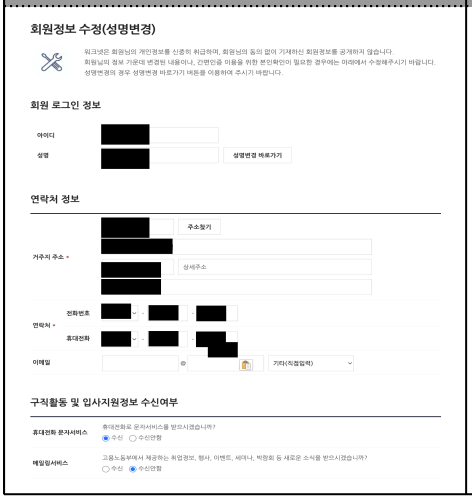
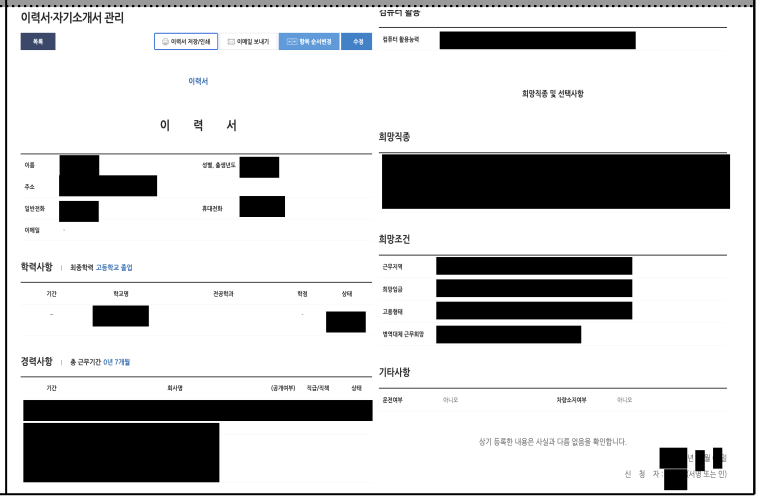
개인정보파일 (시스템명)	수집·이용 항목	수집일	보유건수
구인/구직 관리 (워크넷)	(필수) 성명, 주민등록번호*, 주소, 일반번호, 휴대전화, 성별, 이메일, 학력 (선택) 장애정보, 경력사항, 보유자격, 전산활용능력, 교육훈련 이수현황, 외국어능력, 운전능력, 자기소개서, 해외경험, 여성가장여부, 섬 지역 거주자 여부, 주요활동 및 수상경력, 증명사진, 참여프로젝트, 차량소유여부	'95.1.3.~ '23.7.11.	28,442,085
워크넷 회원파일 (워크넷)	(필수) 아이디, 비밀번호, 성명, 연락처, GPS 위치좌표 (선택) 이메일	'03.07.08.~ '23.05.24.	9,473,560

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

피심인의 시스템(이하 '워크넷') 개인 회원 236,527명의 개인정보가 유출되었고, 유출된 정보에는 '성명, 주소, 일반번호, 휴대전화 번호, 출생년도, 성별, 전자우편, 학력(이상 필수 수집), 경력 사항, 보유 자격, 직업훈련 이수 이력, 외국어 능력, 운전 능력, 해외 경험, 주요활동 및 수상 경력, 증명사진, 참여프로젝트, 차량 소유 여부(이상 선택 수집) 등이 포함되어 있었다.

한편, 피심인은 「고용정책기본법 시행령」 제43조의2제1항에 따라 회원들의 주민등록번호를 처리하고 있으나, 유출된 개인정보 항목에 주민등록번호는 포함되지 않은 것으로 확인된다.

회원정보 수정(성명변경)	이력서·자기소개서 관리 페이지
	

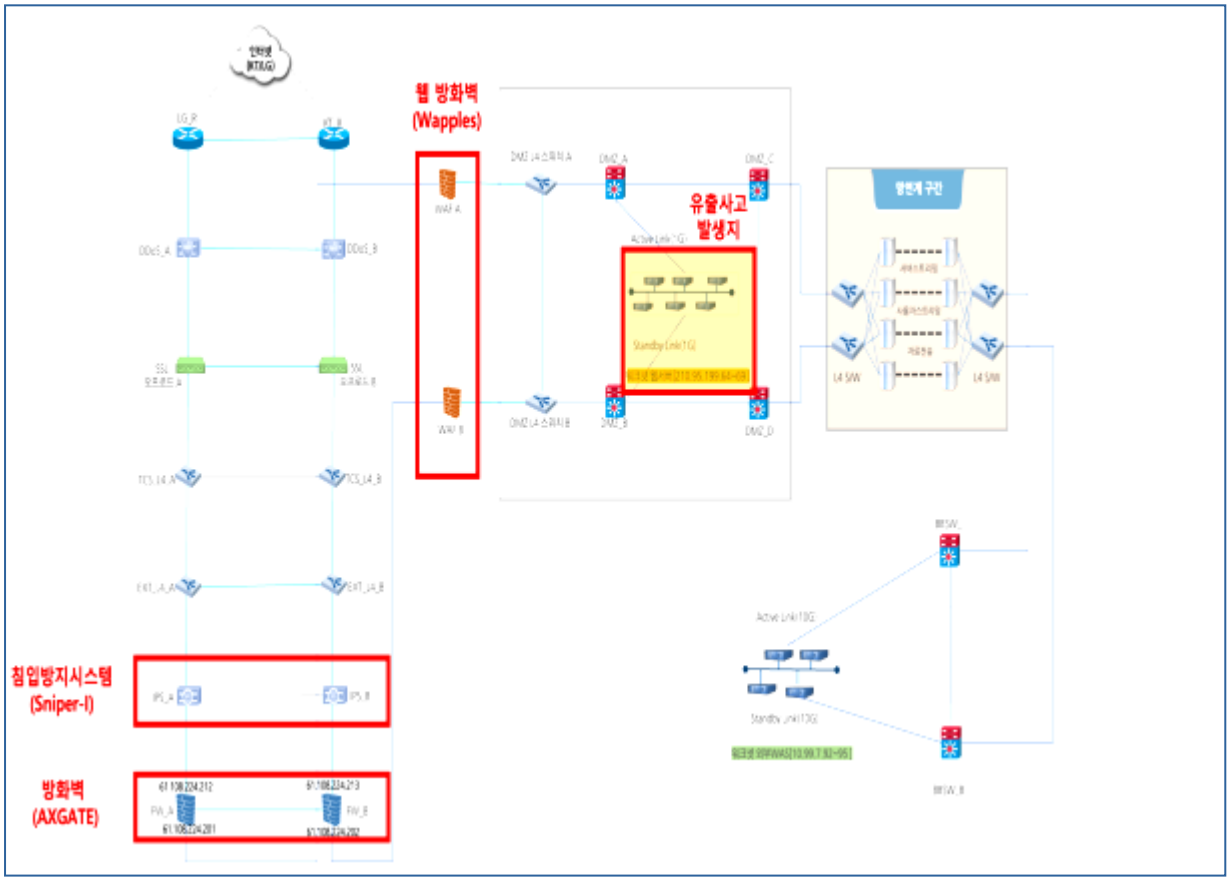
2) 유출인지 및 대응

일시			피심인의 유출 인지·대응 내용
2023.	7. 5.	08:13	워크넷 정상 동작여부 모니터링 솔루션(Jennifer)을 운영하면서, 특정 IP*를 통한 지속적 공격의심 로그인 시도 인지 * 111.25.98.11/32, 122.136.130.7/32, 222.162.142.149/32 등 3개 IP
		08:40 ~ 17:30	다수 로그인 시도 IP 확인 및 방화벽 차단
		10:00 ~ 14:00	신원 미상의 자가 공격의심 IP를 통해 워크넷에 로그인 후 개인정보 화면에 접근한 사실을 확인
		17:42	웹 방화벽(Wapples)을 통해 무차별 대입 공격 차단 * 1초 이내 5회 이상 로그인 시도 시 60초 차단
		20:00	방화벽 차단 IP(총 15개)를 통해 계정정보(ID와 PW) 무차별 대입 방식으로 로그인 후, 내 정보 수정 및 이력서 관리 페이지에 접속한 기록 확인
		24:00	공격의심 접근 확인 IP*(총 26개) 최종 차단 완료 * IP 26개(중국 19, 한국 7)를 통한 로그인 시도 중 5개 IP는 로그인에 실패함
	7. 6.	17:54	한국인터넷진흥원 개인정보 유출 신고
		18:00	개인정보 유출 안내문 워크넷 홈페이지 게시
			개인정보 유출 1차 통지(233,977명*, LMS) * 유출(의심) 236,527명 중 휴대전화번호가 있는 정보주체 233,977명
	7. 7.	16:00	휴대전화번호와 이메일 주소가 확인되지 않는 정보주체 대상 유출 통지서 발송(1명, 우편)
	7. 9.	15:00 ~ 18:00	개인정보 유출 2차 통지(234,539건, 이메일·LMS·유선통화) ※ 미통지: 1,987명(전화, 이메일 등 연락처 없음 1,789명, / 탈퇴회원 198명)

3) 유출 경위

신원 불상의 자가 불상의 방법으로 아이디와 패스워드를 획득한 후 다른 사이트에서도 이를 동일하게 사용하였을 것이라는 전제하에 프로그램을 활용하여 성공할 때까지 로그인을 시도하거나 패스워드에 약간의 변화를 주어 로그인을 시도하는 '크리덴셜 스터핑' 방식을 이용하여, '23. 6. 29. ~ 7. 5. 피심인의 시스템에 불법적으로 접근하였고, 국내외 26개 IP(중국 19개, 한국 7개)를 통해 총 45,110,745회 로그인을 시도하여 21개 IP(중국 15개, 한국 6개)를 통해 564,134회(중복 제거시 236,527회) 로그인에 성공(성공률 1.25%)하였으며, 이 과정에서 1분당 홈페이지 로그인 시도 횟수가 최대 9,997회(평균 4,385회, 초당 73.08회)까지 급증하였다. 로그 분석 결과 신원 불상의 자는 해당 공격을 통해 홈페이지의 '회원정보 수정(성명변경)' 페이지에 482,619회 접근하였고, '이력서·자기소개서 관리' 페이지에 482,408회 접근한 사실을 확인하였다.

※ 시스템 네트워크 구성도



3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보의 안전성 확보조치를 소홀히 한 행위

피심인은 1분당 로그인 시도 횟수가 최대 9,997회(1초당 166회)까지 증가하는 등 비정상적인 로그인 시도가 급증하였음에도, 로그인을 대량으로 시도하는 IP에 대해 탐지만 하고, 즉시 차단하는 조치를 취하지 않은 사실이 있다. 피심인이 보유한 침입방지시스템(Sniper-I)은 1초 이내 32회 로그인이 시도될 경우 이를 탐지할 뿐만 아니라 차단할 수 있는 기능을 가지고 있으나, 피심인은 '23. 7. 5. 이전까지 탐지 정책만 운영하였으며, 피해 발생 이후 '23. 7. 5. 17:42경 웹방화벽(Wapples)을 통하여 '1초 이내 5회 이상 로그인 시도시 60초 차단' 정책을 적용한 사실이 있다.

나. 주민등록번호를 안전하게 보관하지 않은 행위

피심인은 한국법무보호공단으로부터 허브일자리 참여자의 주민등록번호를 수신하고 있으나, 시스템 연계서버(10.99.15.219)에 주민등록번호를 암호화하지 않고 평문으로 저장한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 10. 24. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였고, 피심인은 2023. 11. 8. 개인정보보호위원회에 아래와 같이 의견을 제출하였다.

피심인은 워크넷 운영을 시작한 '98. 11월부터 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위하여 웹 방화벽(Wapples), 방화벽(AXGATE), 침입방지시스템(Sniper-I) 등을 운영하고 있고, 피심인의 시스템은 개인·기관·단체(대학교,

직업학교, 평생교육원 등 교육기관)를 통한 동시다발적 접속을 예정한 구직·구인 정보와 직업·진로 정보를 제공하는 대국민 고용노동서비스로서, 종래에도 정상적인 로그인 시도가 초당 60~70회 수준으로 이루어진 바 있어, 이러한 서비스 특성을 감안할 때 21개의 IP를 이용하여 분당 최대 9,997회(평균 4,385회), 초당 최대 166회(평균 73.08회) 수준의 로그인 시도를 비정상적인 접근 시도로 보기 어려우며, 이로 인한 접근 탐지 및 차단 조치 의무가 발생하였다고 보기 어렵다고 소명하였다.

추가로 피심인은 26개의 IP는 모두 차단하였고, 로그인 시 아이디·비밀번호 외 성명을 추가 입력하고, 사고 이후 최초 접속시 비밀번호를 변경해야만 로그인이 가능하도록 로그인 방식을 변경하는 등 재발 방지 대책을 시행하였으며, 개인정보보호인증(ePRIVACY) 취득, 개인정보 관리수준진단 양호 등급 획득 등 개인정보 보호 노력을 참작하여 선처하여 줄 것을 요청하였다.

Ⅲ. 위법성 판단

1. 관련 법 규정

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 있고, 같은 법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.”라고 규정하면서 “개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)”를 규정하고 있다.

「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호, 이하 ‘舊 고시’) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및

침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.”라고 규정하면서 “개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응(제2호)”을 규정하고 있다.

舊 보호법 제24조의2제2항은 “개인정보처리자는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보의 안전성 확보 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무) 중 접근통제]

개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하고 대응하여야 하며, 이러한 보호조치를 이행하였는지 여부는 보편적으로 알려져 있는 정보보안의 기술수준, 개인정보처리자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹 기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등 사정을 종합적으로 고려하여 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다.(대법원 2018. 1. 25. 선고 2014다203410 판결 참조)

피심인은 웹 방화벽(Wapples), 방화벽(AXGATE), 침입방지시스템(Sniper-I) 등을 운영하고 있으며, 이 중 침입방지시스템(Sniper-I)은 1초 이내 32회 로그인이 시도될 경우 이를 탐지할 뿐만 아니라 차단할 수 있는 기능을 가지고 있으나, 피심인은 ’23. 7. 5.이전까지 탐지 정책만 운영하여 이상 접속 16,326건을 탐지

하는데 그쳤을 뿐 이에 대한 대응 정책은 별도로 적용하지 않는 등 본건과 같은 크리덴셜 스터핑 공격에 대해 효과적으로 대응할 수 있는 형태의 보안 정책을 운영하지 않았으며, 피해 발생 이후 별도 경제적 비용 발생 없이 7. 5. 17:42경 웹방화벽(Wapples)을 통하여 '1초 이내 5회 이상 로그인 시도시 60초 차단' 정책을 적용하는 등 정책을 보완한 사실이 확인된다.

또한 원래부터 피심인의 시스템에 개인·기관·단체의 동시다발적 접속이 많았고, 소명되지는 않았으나 피심인의 주장대로 정상적인 로그인 시도가 초당 60~70회 수준에 달한 전력이 있었다 하더라도, 단시간 내 대량의 접속 실패를 동반하는 것은 정상적인 이용자들의 접속 형태가 아님을 충분히 의심할 수 있고, 평소 로그인 시도에 대한 분석 자료가 없는 상황에서 분당 최대 9,997회(평균 4,385회), 초당 최대 166회(평균 73.08회) 수준의 로그인 시도는 비정상적인 접근으로 간주하여 대응하여야 할 사안으로 판단된다. 추가로 법원에서는 특정 IP의 반복 로그인 시도가 초당 29건 이하인 경우를 악의적인 행위로 판단한 사례가 확인된다.(서울고등법원 2020.11.4. 선고 2019누43964 판결 참조)

IP 주소 대역에 대한 보안 정책을 강화할 경우 정상적인 접근까지 공격으로 잘못 탐지할 여지가 없는 것은 아니나, 피심인은 본건 개인정보파일을 통해 총 3,700만여건의 개인정보를 취급하는 만큼 공공기관 중에서도 높은 수준의 보호조치가 필요하며, 취급하는 개인정보에는 성명·주소 등 기본 사항 외 개인 신상에 관한 광범위한 항목들이 포함되어 있어 불법적인 접근을 탐지·차단할 필요성이 더욱 크므로, 오탐 가능성 및 서비스 편의성 저하 등을 이유로 보안 정책 '룰 세팅' 수준을 완화하는 것은 적절하지 않다고 판단된다.

결국 크리덴셜 스터핑 공격에 대한 방어 여부는 보안 '룰 세팅'을 어떤 수준으로 하느냐에 달려 있는데, 시스템의 특성을 감안하여 초당 로그인 시도가 증가하는 시기 및 횟수 등에 대한 분석을 통해 시스템 보안 정책의 임계치를 조정하거나 정책을 변경하는 방법을 검토하였다면 본건과 같은 피해 발생을 회피할 가능성이 있었다고 판단되나 피심인은 이에 대한 증빙자료는 제출하지

않은 바 있다. 상기 사정들을 종합적으로 고려할 때 피심인이 사회통념상 합리적으로 기대 가능한 정도의 보호조치 의무를 다하였다고 보기 어렵다.

위와 같은 사유로 피심인이 크리덴셜 스터핑을 통한 로그인 시도를 탐지하였음에도 불구하고 차단 조치를 취하지 않아, 회원 236,527명의 개인정보가 유출되도록 한 행위는 舊 보호법 제29조, 같은 법 시행령 제30조제1항, 舊 고시 제6조제1항을 위반한 것이다.

나. 주민등록번호를 안전하게 보관하지 않은 행위

[舊 보호법 제24조의2(주민등록번호의 처리 제한)제2항]

개인정보처리자는 취급하는 주민등록번호를 암호화하여 안전하게 보관하여야 하나, 피심인이 행정정보공동이용센터 서버(10.99.15.219)에 저장되는 허브 일자리 참여자의 주민등록번호를 평문으로 저장한 행위는 舊 보호법 제24조의2제2항을 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조 및 제24조의2제2항 위반행위에 대해 같은 법 제75조제2항제6호·제4의3호, 같은 법 시행령 제63조의 [별표2] 및「舊 개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보위 2023. 3. 8. 이하 '舊 과태료 부과 지침')에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊 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 제29조 및 제24조의2제2항 위반행위에 대해 1회 위반에 해당하는 과태료인 1,200만 원(각 600만 원)을 적용한다.

< 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
카. 법 제24조의2제2항을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제4의3호	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 [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 舊 보호법 제29조 및 제24조의2제2항 위반행위는 舊 과태료 부과지침 제8조의 과태료 가중기준에 해당하지 않아 기준금액을 유지한다.

2) 과태료의 감경

舊 과태료 부과지침 제7조는 “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, ▲사업 규모, ▲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 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 시정 완료하고, 조사 기간 중 행위 사실을 인정하면서 자료 제출 등 조사에 적극 협력하였으며, 개인정보 보호 마크 인증(e PRIVACY)를 받았으므로, 舊 과태료 부과지침 제7조 [별표1] 감경기준에 따라 기준금액의 30%인 360만 원을 감경한다.

< 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	
개인정보 보호노력	7. 위반행위자가 민간자율의 개인정보보호 마크 인증(e PRIVACY PLUS, PRIVACY 등)을 받은 경우	기준금액 20% 이내	

다. 최종 과태료

피심인의 舊 보호법 제29조 및 제24조의2제2항 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 840만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만 원	-	180만 원	**420만 원**
주민등록번호 처리 제한 위반 (암호화 위반)	600만 원	-	180만 원	**420만 원**
계	1,200만 원	-	360만 원	**840만 원**

2. 개선 권고

피심인은 대량의 개인정보를 처리하는 공공기관으로서 높은 수준의 보호조치가 필요하다고 판단되므로 개인정보 보호를 위하여 舊 보호법 제61조제2항에 따라 다음과 같이 개선을 권고한다.

가. 피심인은 시스템의 특성을 감안하여 각종 불법적인 접근 시도 가능성에 대비할 수 있도록 임계치 분석·조정 등 시스템 보안 정책 전반을 정비한다.

나. 피심인은 연계 서버를 포함한 시스템 전반의 주민등록번호 보관 상황을 점검하고, 주민등록번호가 유출되지 아니하도록 암호화하여 안전하게 보관한다.

다. 피심인은 가.부터 나.까지의 개선권고에 따른 조치를 이행하고, 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

3. 결과 공표

舊 보호법 제66조제1항 및 「舊 개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 舊 보호법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우에 해당하므로 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호위원회 처분결과 공표기준」(2023. 10. 11. 개인정보보호위원회 의결)에 따라 공표 기간은 1년으로 한다.

한편, 피심인은 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침('23.10.11. 시행)」 제3조 및 제6조를 근거로 본건 위반행위가 공표(명령) 대상이 아니라고 주장하나, 같은 지침 부칙 제2조에 따르면 "'23. 9. 15. 이전에 종료된 위반행위에 대해서는 종전 「개인정보 보호위원회 처분결과 공표기준」의 제2조에 따른다"라고 규정하고 있으므로 공표 대상에 해당한다.

개인정보 보호법 위반 행정처분 결과 공표 개인정보 보호법 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	한국고용정보원	舊보호법 제29조	안전조치의무 위반	2024.1.24.	과태료 420만 원 개선권고
		舊보호법 제24조의2 제2항	주민등록번호 암호화 미조치		과태료 420만 원 개선권고
2024년 1월 24일 개 인 정 보 보 호 위 원 회					

Ⅴ. 결론

피심인의 舊 보호법 제29조 및 제24조의2제2항 위반행위에 대하여 같은 법 제75조제2항 및 제66조제1항에 따라 주문과 같이 의결한다.

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(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.

이상과 같은 이유로 주문과 같이 의결한다

2024년 1월 24일

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 조 소 영 (서 명)