개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2023-013-169호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2023. 7. 26.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 21,600,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 개선을 권고한다.

   가. 피심인이 보유한 개인정보처리시스템 전반에 대해 점검한다.

   나. 개인정보 보호체계(거버넌스) 및 관련 매뉴얼을 정비하고, 개인정보취급자에 대한 교육을 강화한다.

   다. 개선권고 통지를 받은 날로부터 60일 이내에 조치결과를 제출한다.

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표 한다.

이 유

Ⅰ. 기초 사실

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

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 (이하 ’피심인‘)이 ’22년 11월 실시한 개인정보( )를 유출하여 개인정보 관리실태에 대한 조사(’23. 2. 21. ~ 6.13.)를 실시하였으며, 피심인의 보호법규 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 매년 를 주관·실시하면서, ‘ ’(, ‘ ’)을 통해 아래와 같이 개인정보를 처리하고 있었다.

개인정보파일 (시스템명)	수집·이용 항목	목적	수집 방법	수집보유일 (평가~성적출력)	보유 기간	보유 건수

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

이름, 학교명, 학년, 반, 번호, 성별, 등
의 개인정보 총 2,966,485건이 유출되었다.

당초에는 시행된 에 응시한 들의
270,360건*(충남·경남 제외)이 유출된 것으로 파악하였으나,

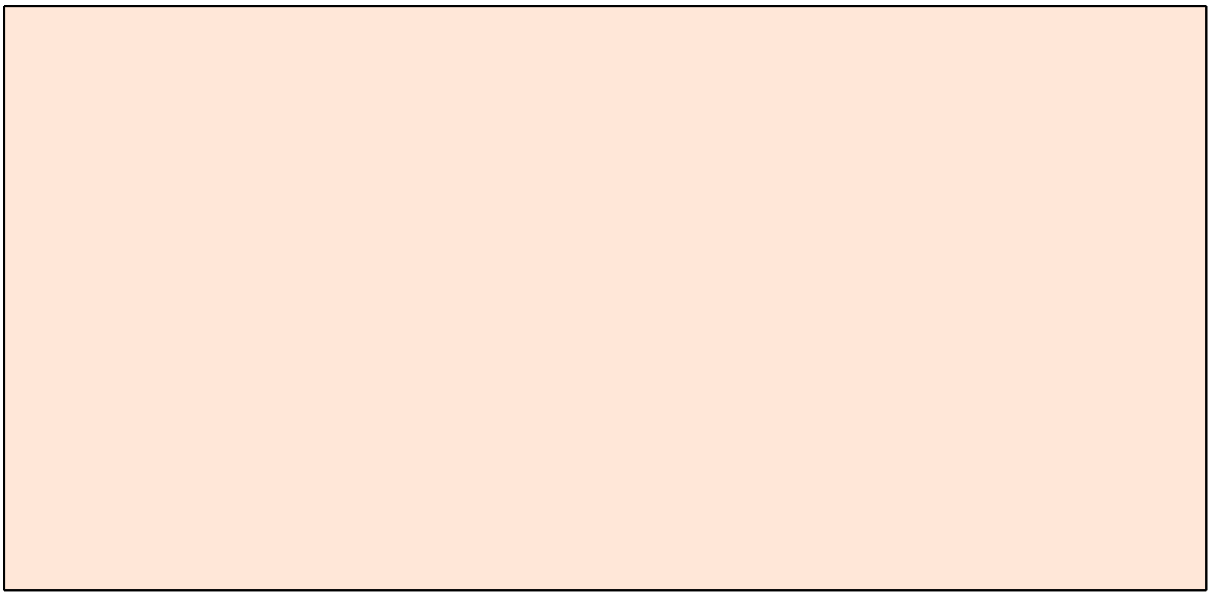
* 신원 미상의 자가 파일 다운로드 후 최초 유포자(텔레그램방 운영자)에게 전달

※ **유출** 초기(2~3월) 디시인사이드 등 **인터넷 커뮤니티로** 성적정보가 **공유·확산됨**

사실 조사 후 , , 각 , 시행된
( )의 성적정보 2,696,125건*(당초 확인 건 미포함)이 추가로 확인 되었다.

* 경찰·교육부 등의 조사과정에서 확인된 것으로, **온라인 유포 정황은 없음**

< 유출 확산 방지를 위한 우리 위원회 조치사항 >



2) 유출 인지 및 대응

일시			유출 인지·대응 내용
'23.	2.18.	22:27	텔레그램에 이 유포됨
	2.19.	00:24	인터넷 커뮤니티(디시인사이드)에 유포 사실이 게시됨
		10:28	언론사 기자 제보를 통해 **유출사실 인지(1차)**
		12:06	온라인시스템 웹사이트( ) 폐쇄
	2.19.~3.30.		홈페이지에 유출사실 게재(1차)
	2.20.	14:47	개인정보보호포털에 **유출 신고**(1차)
	2.21.	21:24~	정보주체에게 **유출 통지**(가정통신문)
	3.14.		온라인시스템을 폐기하고 성적처리 등 업무를 에 위탁 결정
	5.2.		공문 수신을 통해 **추가 정보 유출사실 인지**
	5.3.	20:38	개인정보보호포털에 **유출 신고**(2차)
		23:50~	홈페이지에 유출사실 게재(2차)
	5.4.	09:38~	정보주체에게 **유출 통지**(가정통신문, 홈페이지 게재)

3) 유출 경위

신원 미상의 자가 , 등 누구나 접근 가능한 온라인시스템 공용 게시판에서 일반 게시글의 첨부파일 URL을 확인*하고, 해당 URL의 파일 식별번호(첨부파일ID)를 변경, 인터넷 주소창에 무작위 대입 시도함으로써 성적파일을 다운로드하였다.

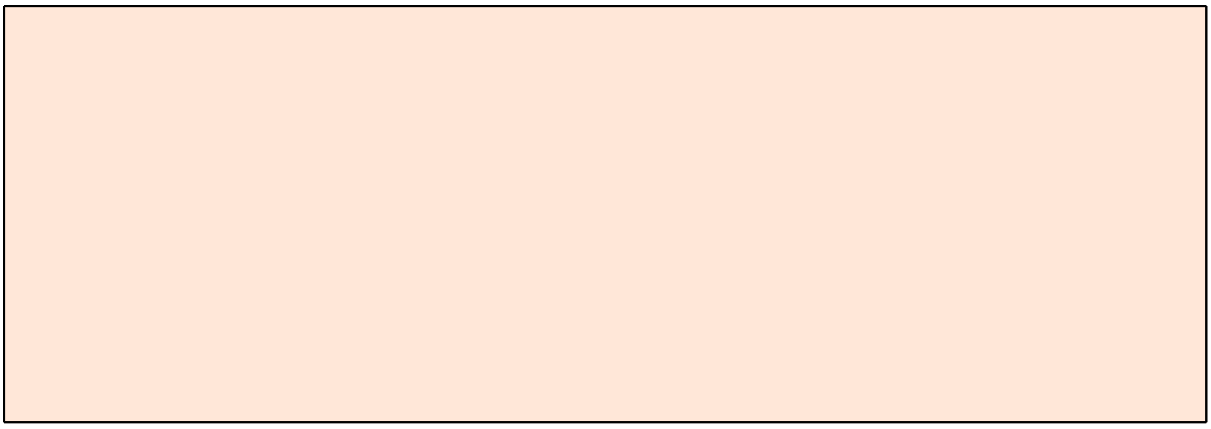
* **온라인시스템 게시판의 파일 다운로드 링크에 커서를 올려놓으면 URL이 표출됨**

(URL 예시)
www. . .kr/cmm/fms/FileDown.do?atchFileId=FILE_**000000000001076**&fileSn=0
(고정값) **(파일 식별번호)** (고정값)

<인터넷 주소창 입력 예시>

【참고사항】

< 개인정보 유출사고 관련 경찰 수사 결과 >



다. ‘ ’이 보호법상 민감정보에 해당하는 지 여부 추가 검토

보호법 제23조는 민감정보에 대한 정의를 두는 대신 민감정보의 종류를 열거하고 있으며, 이에 대해 보호법 해설서(157~164쪽)는 보호법령이 민감정보의 대상을 한정적으로 열거하고 있는 것이라는 취지로 설명하고 있어, 이 사건 ‘ ’의 경우 바로 보호법 상 민감정보로 판단하기 곤란한 측면이 있다.

- 보호법 23조에 따른 민감정보의 종류 : **① 사상·신념 ② 노동조합·정당의 가입·탈퇴 ③ 정치적 견해 ④ 건강, 성생활 등에 관한 정보 ⑤ 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령이 정하는 정보**
- 시행령 제18조에 따른 민감정보의 종류 : **⑥ 유전정보 ⑦ 범죄경력에 관한 정보 ⑧ 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보 ⑨ 인종이나 민족에 관한 정보**

라. 개인정보의 취급·운영 관련 사실관계

1) 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 온라인시스템에 대한 접근권한이 없는 자가 인터넷 주소창에 특정 URL(도메인 + 파일 다운로드 기능을 호출하는 문자열 + 첨부파일ID)을 입력하는 것만으로 서버에 저장된 성적파일이 다운로드 되는데 대해 접근통제 조치를 취하지 아니한 사실이 있다.

※ 온라인시스템에 사용된 전자정부 프레임워크 공통컴포넌트에 URL의 첨부파일ID를 변경하여 서버에 업로드 된 파일에 임의 접근할 수 있는 보안 취약점이 존재하였음

피심인은 개인정보취급자(webmaster 계정)가 외부에서 온라인시스템에 접속할 때, 안전한 접속수단이나 인증수단을 적용하지 않고 아이디·비밀번호만으로 접속할 수 있게 운영한 사실이 있다.

온라인시스템에 사용된 전자정부 공통컴포넌트 제작기관인 표준프레임워크 센터가 보안 취약점*에 대해 '22.12.30. 패치를 공지** 하였음에도, 피심인은 '23.2.18.(성적파일 최초 유포 시점) 까지도 시스템에 보안 업데이트를 하지 아니한 채 운영한 사실이 있다.

* 유추 가능한 첨부파일ID로 인해 타인의 첨부파일 유출 가능

** 표준프레임워크포털(www.egovframe.go.kr) 공지사항 211번 게시물

피심인은 온라인시스템의 관리자페이지 로그인창*에서 아이디와 비밀번호를 일정 횟수 이상 잘못 입력한 경우, 접근을 제한하는 기술적 조치를 취하지 아니한 사실이 있다.

* www. . .kr/uat/uia/loginusr.do

피심인은 온라인시스템 구축시부터 현장조사일까지 접속기록을 점검하지 않았다.

2) 보유기간이 경과된 개인정보를 파기하지 않은 행위

피심인은 보유기간이 경과한 개인정보(2,328,045건)를 파기하지 아니한 사실이 있다.

※ 피심인은 DB에 저장된 정보만 삭제하고 WAS에 저장된 원본 파일을 미삭제

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 5. 16. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 5. 31. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법 규정

보호법 제29조는 “개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 조치를 하여야 한다.”라고 규정하고 있고, 보호법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호), 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호) 및 개인정보에 대한 보안프로그램의 설치 및 갱신(제5호)을 하여야 한다”라고 규정하고 있다.

또한 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 ‘고시’) 제5조제6항은 “개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.”, 제6조제2항은 “개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.”, 제6조제3항은 “개인정보처리자는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.”라고 규정하고 있으며, 제8조제2항은 “개인정보처리자는 개인정보의 오 · 남용, 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손 등에 대응

하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다.", 제9조제2호는 "개인정보처리자는 악성프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치 · 운영하여야 하며, 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시하여야 한다." 라고 규정하고 있다.

나. 위법성 판단

개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 하여야 하나,

1) 피심인이 온라인시스템에서 특정 URL을 인터넷 주소창에 입력하는 것만으로 파일이 다운로드 되는 데 대해 아무런 접근통제 조치를 하지 않은 것은 보호법 제29조, 시행령 제30조제1항 및 고시 제6조제3항 위반에 해당하고,

2) 온라인시스템의 관리자페이지 접속 시 아이디와 비밀번호만으로 접속 가능하도록 운영한 것은 보호법 제29조, 시행령 제30조제1항 및 고시 제6조제2항 위반에 해당하고,

3) 전자정부 공통컴포넌트 제작기관인 표준프레임워크센터가 보안패치를 공지 하였음에도('22.12.30.), 온라인시스템에 즉시 보안 업데이트를 실시하지 않은 것은 보호법 제29조, 시행령 제30조제1항 및 고시 제9조제2호 위반에 해당하고,

4) 온라인시스템의 관리자페이지 로그인창에서 아이디와 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하는 기술적 조치를 취하지 아니한 것은 보호법 제29조, 시행령 제30조제1항 및 고시 제5조제6항 위반에 해당하며,

5) 온라인시스템에 대한 접속기록을 점검하지 아니한 것은 보호법 제29조, 시행령 제30조제1항 및 고시 제8조제2항 위반에 해당한다.

2. 보유기간이 경과된 개인정보를 파기하지 않은 행위

가. 관련 법 규정

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

나. 위법성 판단

개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 하나, 피심인이 보유기간이 경과된 정보를 파기하지 아니한 것은 보호법 제21조제1항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제21조제1항 및 제29조 위반행위에 대해 같은 법 제75조제2항제4호·제6호, 같은 법 시행령 제63조의 [별표2]「과태료의 부과기준」에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 보호법 제29조와 관련하여 최근 3년간 같은 위반행위로 과태료 처분*을 받은 사실이 있으므로 2회 위반에 해당하는 금액 1,200만 원을 적용하고, 제21조제1항과 관련하여 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 금액 600만 원을 적용한다.

* 피심인은 ’21.9.8. 보호법 제29조 위반으로 과태료 480만원 부과 처분을 받음

< 과태료 부과기준, 보호법 시행령 제63조 [별표 2] >

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
마. 법 제21조제1항·제39조의6을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제4호	**600**	1,200	2,400
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 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」(개인정보위 2023. 3. 8. 이하 '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.

보호법 제29조 위반행위에 대하여 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상인 점과 그밖에 위법행위의 결과 등을 고려하여 기준금액의 20%인 240만 원을 가중하고,

보호법 제21조제1항 위반행위에 대해서 법 위반상태의 기간이 3개월 이상인 점과 그 밖에 위법행위의 결과 등을 고려하여 기준금액의 20%인 120만원을 가중한다.

< 과태료 가중기준(제8조 관련) >

기준	가중사유	가중비율
위반의 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우	기준금액의 50% 이내
위반 기간	법 위반상태의 기간이 3개월 이상인 경우	기준금액의 50% 이내
기타	그 밖에 위반행위의 정도, 위반행위의 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우	기준금액의 10% 이내

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 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 과태료 부과지침 제7조 [별표1] 감경기준에 해당 사항이 없어 기준금액을 유지한다.

이와 관련하여 피심인은 이번 사건이 ①시스템 오류로 인하여 발생한 점, ②유출 인지 즉시 온라인시스템을 차단하여 추가 유출을 방지하였고, 유출 확산 방지 및 유출정보 삭제조치를 하였던 점, ③조사 기간 중 적극적으로 협조한 점 등을 고려하여 선처를 요청하였으나,

개인정보위는 ①피심인에게 보안패치 유무 확인 및 적용 의무가 있는 점, ②위반행위 중지 시점에 이미 유출된 성적정보가 인터넷에 광범위하게 유포되어 있던 점, ③유지보수 업체의 비협조로 위법성 판단에 도움이 되는 자료 확보에 어려움이 있었던 점 등을 종합 고려하여 참작의 여지가 없는 것으로 판단하였다.

라. 최종 과태료

피심인의 보호법 제29조 및 제21조제1항 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 2,160만원의 과태료를 부과한다.

< 과태료 산출내역 >

개인정보 보호법		과태료 금액 (단위:만 원)			
위반조항	처분 조항	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제21조제1항	제75조제2항제4호	600	120	-	**720**
제29조	제75조제2항제6호	1,200	240	-	**1,440**
계		1,800	360	-	**2.160**

3. 개선 권고

보호법 제61조제2항에 따라 피심인에게 다음과 같이 개선을 권고한다.

1) 피심인이 보유한 개인정보처리시스템 전반에 대해 점검한다.

2) 개인정보 보호체계(거버넌스) 및 관련 매뉴얼을 정비하고, 개인정보취급자에 대한 교육을 강화한다.

3) 개선권고 통지를 받은 날로부터 60일 이내에 조치결과를 제출한다.

4. 처분 결과의 공표

보호법 제66조제1항에 따라 피심인이 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

*** 개인정보 보호위원회 처분결과 공표기준**
제2조(공표요건) 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우 처분결과를 공표할 수 있다.
4. 법 제75조제2항 각호에 해당하는 위반행위를 2개 이상 한 경우
5. 위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우

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		법 제21조 제1항	개인정보 미파기	2023.7.26.	과태료 720만 원
		법 제29조	안전조치의무 위반		과태료 1,440만 원

2023년 7월 26일
개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 보호법 제29조 및 제21조제1항 위반행위에 대하여 같은 법 제75조제2항, 제61조제2항 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.

2023년 7월 26일

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 홍 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)