

개인정보위, 안전조치 의무 위반 2개 사업자에 38억 8,500만 원 과징금 부과

- 관행적인 회원가입 기능 재검토 및 개인정보 수집을 최소화하고, 개인정보 유출 예방을 위한 웹 취약점 점검, 이상행위 탐지 강화 등 당부

개인정보보호위원회(위원장 송경희, 이하 ‘개인정보위’)는 10월 28일(목) 제21회 전체회의를 열고, 개인정보 보호 법규를 위반한 2개 사업자*에 대해 총 38억 8,500만 원의 과징금을 부과함과 동시에 시정명령 및 공표명령하기로 의결하였다.

- * **주식회사 대교** : 눈높이, 차이홍 등 온·오프라인 종합 교육 서비스 운영 사업자
의료법인 영훈의료재단(대전선병원, 유성선병원) : 의료 서비스 제공 사업자

개인정보위는 개인정보 유출 신고에 따라 조사한 결과, 이들 사업자는 「개인정보 보호법」에 따른 안전조치 의무를 소홀히 한 것으로 확인되었으며, 구체적인 위반 내용과 처분 결과는 다음과 같다.

< 주식회사 대교 : 과징금 32억 5,500만 원, 시정명령 및 공표명령 부과 >

신원 미상의 자(이하 ‘해커’)는 관계사 홈페이지의 웹 취약점을 이용해 웹셸*을 업로드하고, 2024년 8월과 2025년 2월 두 차례에 걸쳐 악성코드를 실행하였다. 이를 통해, 관계사 웹서버와 연동된 (주)대교의 온라인 교육 서비스(macadamia) 회원 데이터베이스(DB)에서 약 65만 명의 이름, 생년월일, 휴대전화번호, 연계정보(CI) 등 개인정보를 유출하였다.

- * 웹셸 공격 : 특정 웹페이지의 파일 업로드 취약점을 통해 시스템에서 실행가능한 악성코드를 삽입 및 실행하여 관리자 권한 획득, 개인정보 탈취 등을 행하는 공격 기법

개인정보위 조사 결과에 따르면, (주)대교는 관계사 웹서버에서 (주)대교 회원 DB로 직접 연결할 수 있는 불필요한 접근을 허용하고 있었다. 또한, 2024년 8월 첫 유출 발생 당시 보안관제업체로부터 이상행위와 관련된 보안탐지 안내를 받았지만, 상세 분석·차단 등 불법적인 개인정보 유출시도에 대한 탐지와 대응 조치를 소홀히 하였고, 2025년 2월에 동일한 방식의 접근 및 유출이 또 다시 발생하였다.

아울러, (주)대교의 개인정보보호책임자(CPO)가 이번 유출사고의 원인이 된 접근통제 사항 등 개인정보 유출 방지를 위한 내부 관리계획의 이행실태 점검을 소홀히 한 사실도 확인되었다.

이에, 개인정보위는 (주)대교에 과징금 32억 5,500만 원을 부과함과 동시에 개인정보처리시스템에 대한 안전조치 강화 및 전반적인 유출사고 대응체계를 정비할 것을 시정명령하고, 사업자 홈페이지에 처분받은 사실을 공표하도록 명령하였다.

< 의료법인 영훈의료재단(대전선병원, 유성선병원) : 과징금 6억 3,000만 원 부과 >

해커는 2024년 3월 영훈의료재단이 운영하는 병원 홈페이지 내 SQL 인젝션 취약점*을 공격하여 병원 홈페이지 회원으로 가입한 188,481명의 아이디, 비밀번호, 이름, 휴대전화번호, 생년월일 등 개인정보를 유출하였다.

* 웹사이트 입력 칸에 정상적인 값 대신 데이터베이스 명령어를 입력하여 결과를 조회

개인정보위 조사 결과에 따르면, 영훈의료재단은 병원 안내, 게시판 이용, 예약신청 등 병원 운영을 보조하는 홈페이지를 운영하면서, 관행적으로 회원 가입 기능을 구현하여 개인정보를 수집·처리하였다. 또한, 웹 취약점 공격 등을 탐지·차단할 수 있는 웹 방화벽 등을 설치·운영하지 않았으며, SQL 인젝션 등 웹 취약점을 점검하거나, 홈페이지 내 입력값을 검증할 수 있는 프로그램 구현 등을 하지 않았다.

아울러, 회원이 병원 홈페이지 회원가입 시 입력한 비밀번호를 암호화하면서 안전하지 않은 암호 알고리즘을 사용하였고, 솔트 값* 등을 사용하지 않아 일부 비밀번호의 경우 복호화가 가능한 사실도 확인되었다.

* 같은 알고리즘에서 동일 hash 값 방지를 위해 암호화 전 비밀번호에 추가하는 임의의 값

이에, 개인정보위는 영혼의료재단에 과징금 6억 3,000만 원을 부과함과 동시에 개인정보처리시스템에 대한 주기적인 취약점 점검 및 개선 조치를 이행할 것을 시정명령하였다.

< 이번 조사·처분의 의의 >

이번 조사처분은 주요 서비스를 제공하는 시스템뿐 아니라 관계사와 연결된 서버나 주요 서비스의 운영을 보조하는 홈페이지도 개인정보 유출의 경로가 될 수 있음을 확인하고, 관행적으로 수집하는 개인정보에 대한 현황 파악 및 안전조치 점검의 중요성을 강조하였다는 데 의의가 있다.

또한, 보안 위협을 탐지하고도 적절히 대응하지 않거나 내부 관리계획의 이행 여부를 실효적으로 점검하지 않으면 동일한 방식의 개인정보 유출이 반복될 수 있다는 점에서 개인정보보호책임자의 경각심을 높이는 계기가 될 것으로 기대된다.

이에, 개인정보위는 홈페이지 회원가입 기능 등의 필요성을 검토하여 불필요한 개인정보가 수집되지 않도록 조치하고, 운영 중인 개인정보처리시스템 현황을 파악하여 웹쉘이나 SQL 인젝션 같은 잘 알려진 웹 취약점 공격에 대비한 웹 취약점 점검, 이상행위 탐지 및 대응체계를 강화할 것을 당부하였다.

담당 부서 <총괄>	개인정보보호위원회 조사2과	책임자	과 장	이정은 (02-2100-3121)
		담당자	조사관	허재형 (02-2100-3195)
	조사1과	책임자	과 장	윤여진 (02-2100-3111)
		담당자	조사관	고명석 (02-2100-3119)
담당 부서 <공동>	한국인터넷진흥원 유출조사팀	책임자	팀 장	손기종 (061-820-2850)
		담당자	책 임	한상원 (061-820-2853)
		담당자	주 임	나정용 (061-820-2858)



붙임**사업자별 위반 및 시정조치 내역(종합)**

사업자명	위반 내용	위반 조항	시정조치(안)
주식회사 대교	• 안전조치의무 위반 (접근통제, 내부 관리계획 점검)	보호법 §29	• 과징금 32억 5,500만 원 • 시정명령 • 공표명령
의료법인 영훈의료재단	• 안전조치의무 위반 (접근통제, 암호화)	보호법 §29	• 과징금 6억 3,000만 원 • 시정명령