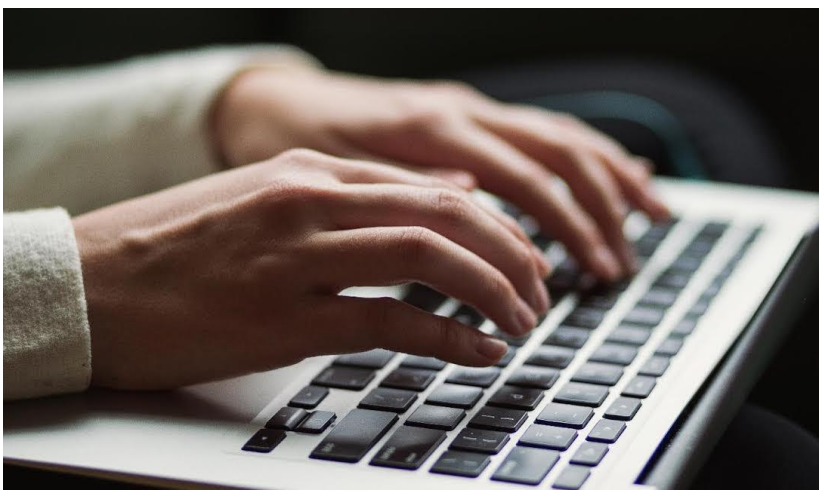
법무법인 린

Newsletter **TMT·정보보호팀** November 2, 2023



개인정보 보호조치 위반과 관련된 과징금 산정의 적법성

– 대법원 2023.10.12 선고 2022두68923판결 분석

1. 개인정보 유출 이유로 부과된 과징금의 적법성

구「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2020. 2. 4. 법률 제16955호로 개정되기 전의 것, 이하 '구 정보통신망법') 제28조 제1항은 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 ① 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립 · 시행 ② 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치 · 운영 ③ 접속기록의 위조 · 변조 방지를 위한 조치 ④ 개인정보를 안전하게 저장 · 전송할 수 있는 암호화기술 등을 이용한 보안조치 ⑤ 백신 소프트웨어의 설치 · 운영 등 컴퓨터바이러스에 의한 침해 방지조치 ⑥ 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치(이하 '개인정보 보호조치')를 하여야 한다고 정하고 있었습니다.

이와 같은 개인정보 보호조치의 이행 확보를 위하여, 구 정보통신망법 제64조의3 제1항 제6호는 정보통신서비스 제공자등이 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 구 정보통신망법 제28조 제1항의 개인정보 보호조치 중 위 ②~⑤를 하지 아니한 경우에는 방송통신위원회가 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다고 정하였습니다.

이와 관련하여, 지난 10월 12일자로 선고된 대법원판결은 개인정보 보호조치 위반을 이유로 부과된 과징금 산정의 범위와 그 적법성 여부를 주요 논점으로 다루고 있습니다. 본 뉴스레터에서는 이 대법원 판결을 구체적으로 살펴봄으로써, 정보통신서비스 제공자(나아가 개인정보처리자)가 개인정보 보호조치 이행과 관련하여 유의할 점을 검토하고자 합니다.

2. 대법원 2023. 10. 12. 선고 2022두68923 판결 요지

웹과 모바일 어플레케이션을 통해 제공되는 온라인 쇼핑몰(이하 '이 사건 쇼핑몰')을 운영하는 주식회사 A(구 정보통신망법 제2조 제1항에 따른 정보통신서비스 제공자)는 2018. 11. 1. 이벤트 대상 상품을 일정 금액 이상 구매하는 경우 사용할 수 있는 포인트 적립권을 선착순으로 배포하는 이벤트(이하 '이 사건 이벤트')를 진행하였습니다. 주식회사 A는 이 사건 이벤트를 준비하면서 이 사건 쇼핑몰의 PC용 웹사이트와 모바일용 웹사이트에 이벤트 페이지를 각각 만들었고, 각각에 대한 별도의 캐시 정책을 마련하였습니다. 이용자에 대한 개인정보의 출력은 '웹서버의 웹 어플리케이션을 통한 데이터베이스서버의 개인정보 요청 → 데이터베이스서버의 웹 어플리케이션을 통한 개인정보의 웹서버 제공 → 웹서버로 전송된 개인정보의 화면 출력'의 단계로 이루어졌습니다.

그러나 주식회사 A는 모바일 웹을 통해 접속 가능한 이 사건 이벤트 페이지의 캐시 정책을 잘못 설정하였고, 그 결과 이 사건 쇼핑몰 이용자 20명의 개인정보가 다른 이용자 29명에게 노출되는 사고(이하 '이 사건 사고')가 발생하였습니다. 이에 방송통신위원회는 주식회사 A가 구 정보통신망법 제28조 제1항 제2호(개인정보 보호조치 중 ②번 내용)을 위반하여 이 사건 쇼핑몰 이용자의 개인정보를 유출했다는 이유로 2019. 12. 27. 주식회사 A에 대하여 각 시정명령, 과태료 및 과징금 18억 5,200만원 등을 부과하였습니다(위 각 처분 중 과징금에 대한 부분은 이하 '이 사건 과징금 처분').

이에 주식회사 A는 이 사건 과징금 처분 취소를 구하였습니다. 1심(서울행정법원 2020구합59628 판결)은 이 사건 과징금 처분이 비례의 원칙에 위배되어 위법하므로 취소하라고 판결하였고, 2심(서울고등법원 2021누73975 판결) 역시 같은 결론을 내렸습니다.

대법원도 1, 2심과 같이 이 사건 과징금 처분이 비례의 원칙에 위배되어 취소되어야 한다고 보면서도, 이 사건 과징금 산정 기준을 이 사건 이벤트로 인한 주식회사 A의 매출액으로 국한하여야 한다고 본 원심의 판단은 법리를 오해한 잘못이 있다고 판단하였습니다.

3. 대법원 2023. 10. 12. 선고 2022두68923 판결의 주요 쟁점

가. 이 사건 과징금 산정의 기초가 되는 매출액의 범위

이 사건 과징금의 구체적 산정기준과 산정절차를 정하고 있는 구 정보통신망 시행령 제69조의2 제1항 본문은 '위반행위와 관련한 매출액'을 "해당 정보통신서비스 제공자 등의 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액"이라고 정의하고 있고, 위 매출액 산정에 관한 세부기준을 정한 구「개인정보보호 법규 위반에 대한 과징금 부과기준」(2020. 12. 10. 방송통신위원회고시 제2020-9호로 폐지되기 전의 것, 이하 '구 과징금 부과기준') 제4조 제1항은 위 매출액을 "위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 직전 3개 사업연도의 연평균 매출액"으로 정하였고, 같은 조 제2항은 관련 매출액 산정 시 서비스의 범위는 서비스 제공방식, 서비스 가입방식, 이용약관에서 규정한 서비스 범위, 개인정보 데이터베이스 관리 조직·인력 및 시스템 운영 방식 등을 고려하여 판단한다고 정하고 있었습니다.

대법원은, 이 사건 과징금은 위반행위에 대한 제재의 성격과 불법적인 경제적 이익을 박탈하기 위한 부당이득 환수로서의 성격을 함께 갖고 있다고 전제하면서, 이용자의 개인정보가 유출된 경우 개인정보 보호조치를 취하지 않아 매출액이 증대되는 경우를 상정하기 어렵고, 구 과징금 부과기준 제4조 제2항에서 정하고 있는 고려사항은 개인정보 보호조치 위반행위로 인하여 취득한 이익의 규모와 직접 관련도 없으므로, 오히려 개인정보 보호조치를 취하지 않은 개인정보를 자신의 영업을 위해 보유함으로써 얻은 이익을 환수할 이익으로 보아, 매출액 산정 시 서비스의 범위는 유출사고가 발생한 개인정보를 보유·관리하고 있는 서비스의 범위를 기준으로 판단하여야 한다고 하였습니다.

더불어, 이 사건 이벤트 페이지를 통해 유출된 개인정보는 이 사건 이벤트 페이지에서 제공하는 서비스만을 목적으로 수집·관리된 정보가 아닌 점, 이 사건 이벤트 페이지는 이 사건 쇼핑몰에서 제공하는 서비스와 구분될 수 없는 점 등을 고려하면, 이 사건 과징금의 관련 매출액은 이 사건 쇼핑몰 서비스 전체의 매출액으로 보아야 한다고 하였습니다.

다만, 대법원은 일반론으로 이 사건 쇼핑몰 이용자들의 개인정보가 담긴 데이터베이스와 관련하여 독립된 접근경로를 가진 웹페이지에서 제공하는 서비스가 이 사건 쇼핑몰이 제공하는 서비스와 외견상 구분되는 독자적인 서비스인 경우에는 해당 서비스에서 발생한 매출액만을 관련 매출액으로 산정할 여지가 있음을 인정하였습니다.

나. 과징금 처분의 재량권의 일탈 남용

대법원은, 구 정보통신망법 제64조의3 제3항은 과징금을 부과할 때 위반행위의 내용과 정도, 기간과 횟수 외에 위반행위로 인하여 취득한 이익의 규모 등도 고려하도록 규정하고 있다고 확인하면서, 개인정보 보호조치 의무 위반에 대해 부과되는 과징금의 액수는 보호조치 위반행위의 원인과 유형, 위반행위로 인해 유출된 개인정보의 규모, 위반행위 방지를 위한 조치의무의 이행 정도, 유사 사례에서의 과징금 액수 등을 종합적으로 고려할 때, 과징금의 액수가 위반행위의 내용에 비해 과중하여 사회통념상 현저하게 타당성을 잃은 경우라면 그러한 과징금 처분은 재량권을 일탈·남용하여 위법하다고 하였습니다.

이에 따라 대법원은, 주식회사 A는 이 사건 이벤트 페이지에 이 사건 사고의 원인이 된 캐시 정책이 적용된 지 하루만에 이 사건 사고를 신고한 점, 주민등록번호·비밀번호 등은 노출되지 않은 점, 이 사건 사고가 구조적인 문제로 인하여 발생하였다고 보기 어렵고 추가 피해 우려도 비교적 작았던 점, 담당 직원의 단순 과실로 비교적 적은 수의 개인정보 유출 사고가 발생한 경우 이 사건 과징금과 같이 거액의 과징금이 부과된 사례는 찾아보기 어려운 점, 구 과징금 부과기준 등 과징금 부과에 관한 세부기준을 보더라도 위반 정도가 경미한 경우 시정조치 명령으로 갈음하거나 과징금을 면제할 수 있다고 정하고 있는 점 등을 고려할 때, (과징금 산정의 기초가 되는 관련 매출액이 이 사건 쇼핑몰 서비스의 전체 매출액으로 보더라도) 이 사건 과징금은 재량권 일탈·남용이 있어 위법하다고 보았습니다.

4. 시사점

가. 개인정보 보호조치 위반시 부과되는 과징금 관련, 매출액 산정 시 서비스의 범위를 판단할 때 유의사항

본 판결은, 개인정보 보호조치를 위반할 때 부과되는 과징금의 성격을 부당이득 환수의 성격을 가진다고 확인하고, 개인정보 보호조치 위반으로 야기되는 유출사고 관련 매출액의 기준을 유출사고가 발생한 개인정보를 보유·관리하는 서비스의 범위로 제시하였다는 의미가 있습니다.

본 판결은 개인정보 유출사고를 야기한 별도 서비스와 본래 서비스가 구분될 수 없는 사안에 관한 것입니다. 대법원이 만약 개인정보 유출사고를 야기한 서비스가 본래 서비스와 외견상 독자적으로 구분될 수 있다면 해당 서비스에서 발생한 매출액만을 관련 매출액으로 산정할 여지가 있다고 보았다는 점은 실무적으로 매우 중요하게 평가되어야 할 것입니다. 대규모의 개인정보를 통합 처리하고 여러 형태의 서비스를 제공하는 사업자는 서비스 설계시 개인정보 데이터베이스를 일부 분리하여 저장하면서 경로상 독립적인 서비스를 제공하는 아키텍쳐를 고려할 필요가 있습니다.

따라서 과징금에 대하여 다툴 시에는 개인정보 유출사고가 발생한 별도 서비스가 본래 서비스와 독립적인지 여부를 중요하게 볼 필요가 있습니다.

이러한 시사점은 아래 다.에서 설명 드리는 개인정보보호법 개정에 의한 과징금 부과 기준 변경에도 불구하고 유효할 것으로 보여집니다.

나. 본 판결에서 위반하였다고 본 개인정보 보호조치 이행을 위한 유의사항

구 정보통신망법 제28조 제1항 제2호(개인정보 보호조치 중 ②번)는 같은 법 시행령 제15조 제2항에 따라 구체화되고, 위 시행령 제15조 제2항은 개인정보

보호조치 대상을 “개인정보처리시스템”(개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템)으로 보고 있습니다.

본 판결에서 다루어지지는 않았으나, 주식회사 A는 1심에서 이 사건 사고를 야기한 캐시 정책은 웹서버에 적용된 것이고 웹서버는 데이터베이스시스템이 아니므로 개인정보처리시스템이 아니어서 개인정보 보호조치 대상이 아니라는 취지로 주장하였습니다.

그러나 1심 판결은 웹서버도 개인정보처리시스템으로 인정하였습니다. '개인정보처리시스템'이란 개인정보의 생성, 기록, 저장, 검색, 이용과정 등 데이터베이스 관리시스템 (DBMS) 및 응용프로그램 전체를 의미하는 것으로 보는 것이 개인정보 보호조치 제도 목적에 부합하고, 이용자 개인정보의 제공·수집이나 개인정보의 제공 역시 웹서버 전송을 통하여 이루어지는 등 이용자 개인정보의 처리를 위하여는 웹서버, 웹 어플리케이션, 데이터베이스서버가 모두 필요한 점, 개인정보에 대한 불법적인 접근의 유형은 데이터베이스서버에 바로 침입하는 유형에 의해서만 이루어지는 것은 아닌 점 등에 비추어 보더라도, 데이터베이스(DB)서버만을 개인정보처리시스템이라고 해석하기 어려운 점 등이 인정되기 때문입니다.

웹서버도 개인정보 보호조치의 대상이 되는 개인정보처리시스템에 포함될 수 있다는 점은 이미 KT 개인정보유출 사건의 상고심에서도 확인된 바 있습니다(대법원 2021. 8. 19. 선고 2018두56404 판결).

따라서 사업자는 개인정보를 직접 다루는 데이터베이스 서버 뿐 아니라, 그 데이터베이스를 관리하거나 용이하게 이용하는데 필요한 부가 시스템·프로그램 및 그 앞단의 웹서버 등도 개인정보 보호조치의 대상이 되는 개인정보처리시스템으로 보고 필요한 조치를 취하여야 합니다.

다. 현행 개인정보보호법과의 비교

본 판결에서 다루어진 구 정보통신망법 규정이 삭제되고 개인정보 보호 관련 규정이 개인정보 보호법에 통합됨에 따라, 2020. 8.5. 이후 개인정보를 처리하는 정보통신서비스 제공자는 개인정보보호법에 따라 개인정보 보호조치를 이행하게 되었습니다. 정보통신서비스 제공자는 현행 개인정보보호법 하에서 본 판결이 어떻게 적용될 지 유념하여야 합니다.

현행 개인정보보호법 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 한다고 정하고 있습니다. 개인정보보호법 시행령 제30조 제1항은 구 정보통신망법령와 동등한 수준의 개인정보처리시스템에 관한 보호조치를 하도록 정하고 있습니다. 따라서, 본 판결에서 다룬 개인정보 보호조치의 수준은 현행 개인정보 보호법에서도 동일하다고 할 수 있습니다.

한편, 2023. 3.14. 개인정보 보호법이 전면 개정되면서 과징금 부과의 기준 및 절차가 변경되었습니다(2023. 9.15.시행). 구 정보통신망법 및 구 개인정보 보호법은 본 판결에서 문제된 위반행위를 포함하여 일정한 유형의 법위반행위에 대한 과징금 상한을 ‘위반행위와 관련한 매출액’의 3/100 이하로 하고 있었으나, 개정 개인정보 보호법은 ‘전체 매출액’의 3/100 이하로 상향 조정하였습니다(제64조의2 제1항). 다만 최초 정부안과 달리 입법과정에서 “개인정보 보호위원회는 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 과징금을 산정한다”는 규정이 추가되어(제64조의2 제2항), 문언해석상 구 법과 어떠한 차이가 있는지 불분명한 점이 발생하였습니다.

이에 대해 개인정보 보호위원회는 전체 매출을 근거로 보호위원회가 과징금을 산정하면 개인정보처리자가 위반행위와 관련없는 매출액을 입증하여 이를 전체 매출액에서 공제하는 구조로 입증책임이 전환된다고 설명하고 있습니다. 행정처분의 적법성은 처분청이 입증해야 하므로 이와 같은 개정이 법률상의 입증책임을 전환하였다고 보기는 어려우나 ‘관련 매출액’의 입증을 위해 사실상 내지 실무상 개인정보처리자의 자료제출의무가 강화되었다고 볼 수 있습니다.

* * *

상기 내용에 관해 문의사항 있으시면 언제든지 저희 법무법인 린의 TMT·정보보호팀 구태언 변호사(Tel. 02-3477-8695)에게 연락 주시기 바랍니다.

홈페이지

관련 구성원

구태언 변호사
T. 02-3477-8695
E. tekoo@law-lin.com

전응준 변호사
T. 02-3477-8695
E. ejjeon@law-lin.com

김호연 변호사
T. 02-3477-8695
E. hykim@law-lin.com

법무법인 린

서울 서초구 서초중앙로 24 길 27, 지파이브센트럴 프라자 326 호
T.02-3477-8695 F.02-3477-8694