2024 개인정보 과징금 5대 이슈

1. **‘전체 매출액 3% 과징금’** 첫 적용
2. **혼선을 통해서 정보주체의 동의를** 유도하는 **‘다크패턴’에 과징금** 최초부과
3. **종교, 정치, 동성혼 등 ‘동의없는 민감정보 수집’** 및 마케팅에 활용한 B사 **216억 과징금**
4. **‘내부관리용 번호’가 다른 정보와 결합**하여 **개인이 식별**될 경우 **과징금 부과대상**
5. **‘오픈소스 취약점’ 조치 미비**에 대한 **최초 과징금** 부과

Privacy Report

2024 개인정보 과징금 5대 이슈

1. **‘전체 매출액 3% 과징금’** 첫 적용
   A사 220만명 개인정보유출 과징금 75억

2. **혼선을 통해서 정보주체의 동의를** 유도하는 **‘다크패턴’에 과징금** 최초부과
   보험사 4곳 과징금 92억

3. **종교, 정치, 동성결혼 등 ‘동의없는 민감정보 수집’** 및 마케팅에 활용한 B사에 **216억 과징금** 부과
   국내 98만명 민감정보를 9만 여 타깃광고에 이용

4. **‘내부관리용 번호’가 다른 정보와 결합**하여 **개인이 식별**될 경우 **과징금 부과대상**
   C사 6만5천명 개인정보 유출 과징금 151억

5. **‘오픈소스 취약점’ 조치 미비**에 대한 **최초 과징금** 부과
   D사 2만2천명 개인정보 노출 과징금 13억

SOMANSA

01

‘전체 매출액 3% 과징금’ 첫 적용

75억원

2023년 9월 개인정보보호법 개정으로
기술적 관리적 보호조치 미흡 등 중대과실로 개인정보가 유출된 경우
‘전체매출의 최대 3%까지 부과’ (개정 전에는 관련 매출의 3% 부과)

- A사 **해킹으로 내부서버 내 개인정보 220만 건 유출**
  - 개인정보파일 점검, 공유설정 안전조치 미흡
  - 주민등록번호 처리 및 개인정보 파기의무 위반
  - 개인정보 유출통제, 악성코드 유입통제 기술적 보호조치 미흡
  - VPN 원격접속 보안통제 미흡 등

  보호조치가 심각하게 미비한 상태였기에 **과징금 75억원 부과**

- 10월 개정발간된 ‘개인정보보호법고시 안내서’에 따라
  FTP, 백업서버 등 공용파일처리시스템도 개인정보 처리시스템으로
  확대되어 DBMS, WAS와 같은 기술적 보호조치 구축 필요

02

혼선을 통해서 정보주체의 동의를 유도하는 ‘다크패턴’에 과징금 최초부과

보험사 4곳 총 92억원

미동의 의사를 표시한 이용자에게 혼선을 일으키는 ‘UI’로 재동의를 받아
해당 방식으로 수집한 정보를 상업적으로 이용한 경우
‘수집 이용 동의 위반’에 따른 과징금 부과대상으로 간주함

- **4개 보험사 총 92억 과징금 부과**
  - 미동의 의사를 표시한 사용자에게 ‘재유도 창’을 노출하여 받은 마케팅 동의율은 기존대비 최대 2배 증가 (31.42% → 61.71%)
  - 수집된 개인정보는 자동차 보험, 운전자보험, 건강보험 등 다른 보험마케팅에 활용 됨
    (특히 자동차보험에 최소 3천만 건 불법 활용된 것으로 추정)

- **CPO(개인정보 최고책임자)**는 적법한 개인정보 처리를 위하여 **내부시스템 구축, 프로세스 확보 등 내부통제 역할**도 수행해야 함

*다크패턴 : 사용자가 특정행동을 하도록 유도하기 위해 교묘히 설계된 사용자 인터페이스(UI)

SOMANSA

03

‘동의없는 민감정보 수집’ 및 마케팅에 활용한 소셜미디어 기업 B사에 과징금 부과

216억원

국내시장 진출 후 다섯번째 개인정보 유출 제재
부과된 과징금 누적 약 729억원

- **국내 98만명 이용자 대상 종교, 정치, 동성결혼여부** 등 민감정보를 **정보주체 동의 없이** 무단수집
- 정보주체의 동의없이 수집된 정보는 **4천 여 광고주에 의해 동성애, 트랜스젠더, 북한이탈주민 등** 민감한 주제로 9만 여 개 **타깃 광고에 이용**
- 2020년(67억), 2021년(64억원), 2022년(308억), 2023년(74억), 2024년(216억)
  B사 국내 처벌 과징금 누적 합산 시 약 729억원 상당

04

‘내부관리용 번호’가 다른 정보와 결합하여 개인이 식별될 경우 과징금 부과대상

151억원

회원 개개인에게 부여된 ‘내부관리용 번호’가
다른 정보와 결합하여 정보주체가 식별된다면
개인정보보호에 관한 기술적 보호조치를 다 하지 않은 것으로 판단됨

- 회원 개개인에게 부여된 '내부관리용 번호’가
  특정 메신저의 익명채팅방 ID에 포함되어 있어,
  익명채팅방 **참여자 모두에게 공개**
- **해커가** 해당 메신저 **프로토콜 취약점**을 활용하여
  ‘내부관리용 번호’를 매개로
  채팅방 참여자의 메신저 프로필 정보와 핸드폰 번호를 추출
- 이후 해당 정보를 **데이터베이스화 하여 판매**
- **약 6만 5천 여 명** 개인정보가 1건당 **5천 내외로 거래**된 것으로 추정
- 개인정보보호위원회가 부과한 **과징금의 최종 확정 여부는**
  향후 소송에 의해 결정될 것으로 추정

05

‘오픈소스 취약점 조치’ 미비에 대한 최초 과징금 부과

13억원

오픈소스 취약점 미조치는 기존 과태료 부과대상 이었으나
2024년 이후부터 과징금 집행으로 변화되고 있음

- 취약점 조치 미비로 국내 최초 과징금을 받은 **D사**는
  오픈소스 특정기능에 취약점 경고가 있었음에도
  점검 및 개선조치를 취하지 않아 개인정보가 노출 됨
- 웹 또는 앱서비스로 대규모 개인정보를 처리하는 사업자는
  ‘데이터 통신 연동 및 오픈소스 취약점’을 주기적으로 점검해야 함
- **플랫폼 기반 기업**은 다수 업체가 이용하는 **공급망을 운영/관리**하므로
  정부는 일정규모 이상 개인정보를 처리하는 기업에게
  위험관리를 위한 **‘SBOM(소프트웨어 자재명세서)’**을 권고하고 있음