# 개정법에 비추어 본 개인정보 관련 주요 리스크와 대응방안

BACK TO BASIC

2024. 6. 5.

변호사 김진환
kim.jh@whaleandsun.com

WHALE & SUN
SPIRIT OF CONSULTATION

# 김 진 환 변호사

법률사무소 웨일앤썬 대표
㈜지키다 대표

## 주요 경력

- 서울지방법원 및 남부지원 판사(1998-2001)
- 김앤장 법률사무소 변호사(2001-2021) : Privacy & Data Security 그룹 리더
- 대법원 산하 사법연수원 외래교수(2000-2013)
- 미국 뉴욕주 변호사(2006-현재)
- 개인정보 보호법 해설서 자문위원(2016) 및 집필위원(2020)
- 개인정보보호위원회 고문변호사(2012-2020, 2022-2023)
- 개인정보분쟁조정위원회 위원(2022-2023)
- 개인정보보호위원회 비상임 위원 (2023-현재)
- 개인정보국외이전전문위원회 위원장(2024-현재)

## 주요 담당 업무

- 옥션, 네이트·싸이월드, 현대카드, 넥슨, KT 1·2차, 카드3사, 빗썸 등 해킹 및 정보유출 사건 등 조사 및 형사 대응, 민형사 행정소송 수행
- 국내외 약 200여개 기업에 대한 자문 및 개인정보 컨설팅·프로젝트 수행

## 주요 저술

- 전자거래법 (공저, 사법연수원, 2000-2013)
- 상법주석 (공저, 사법행정학회, 2001)
- The Privacy, Data Protection and Cybersecurity Law Review (Edition1): Korea Chapter (공저, Law Business Research, 2014)
- 온주(온라인 주석서) 정보통신망법, 전자문서법, 전자서명법 (공저, 로앤비, 2017, 2019, 2023)
- 개인정보보호법 (공저, 박영사, 2024)

## 주요 수상

- 개인정보보호 대상 : 국회 행정안전위원회 위원장상(2012), 개인정보 : 안전행정부 장관 표창(2013)
- Leading Lawyer : IT, Telecommunication & Media(Asia Law & Practce, 2014, 2016, 2018)
- Leading Individual, Asialaw Profiles(Euromoney, 2017)
- 개인정보 : 국민포장(2022)

# 목차

- 개정 개인정보 보호법의 주요 개정사항
- 개인정보처리자인 기관의 각종 리스크
- 개인정보처리자인 기관의 Back-to-Basic 대응방안

# 개정 개인정보 보호법의 주요 개정사항

# 개정 개인정보 보호법의 주요 개정사항 1

- **이동형 영상정보처리기기 운영 기준 마련**

  ① 고정형 vs. 이동형 구별; ② 불빛, 소리, 안내판 등으로 명확히 표시 후 거부의사 부재시

- **동의를 포함한 개인정보의 수집·이용 방법 개선**

  ① 목적 내 제공에 정당한 이익 추가; ② 필수 동의(제) 폐지; ③ 마케팅 “구분” 동의

- **개인정보의 국외 이전 다양화 및 국외 이전 중지명령 신설**

  ① 인증 획득 경우와 인정제 추가; ② 국외 이전 중지명령과 재이전 규제

- **개인정보 처리방침의 평가 및 개선권고**

  ① 기재 사항 누락 여부; ② 이해하기 쉽게 작성; ③ 쉽게 확인할 수 있도록 공개

- **개인정보의 전송 요구권 신설**

  ① 일반적 마이데이터제도; ② 시행 시기 미정; ③ 수범자의 범위 등 주요 사항 시행령 위임

- **자동화된 결정에 대한 정보주체의 권리 신설**

  ① AI 포함 완전히 자동화된 시스템; ② 권리/의무에 중대한 영향; ③ 거부권, 설명요구권

# 개정 개인정보 보호법의 주요 개정사항 2

- **개인정보 보호책임자의 업무·자격요건 보완 및 독립성 보장 신설**

  ① 미지정시 사업주/대표자; ② 독립적 업무수행 보장 ; ③ 자격요건 강화

- **징벌적 손해배상액 및 보장 보험 등 가입 의무 확대**

  ① 5배 손해까지 배상; ② OSP 외 일반 개인정보처리자에 보험 및 적립금제 확대

- **개인정보 분쟁조정제도 개선**

  ① 의무적 조정제도 대폭 확대; ② 조정위의 사실조사권 인정; ③ 이의 부제기시 조정 수락 의제 신설

- **과징금 규정 정비**

  ① 과징금 부과 대상 대폭 확대; ② 과징금 부과 기준 확대(전체 매출액 vs. 관련 매출액)

- **개인정보 보호수준 평가제 실시**

  ① 1,600여개 공공기관으로 확대; ②정량 : 정성 = 60 : 40

- **수탁자에 대한 행정 제재 및 형사 처벌 규정 추가**

  ① 과태료 및 과징금에 명문화; ② 형사처벌 규정에 명문화

# 개인정보처리자인 기관의 각종 리스크

# 개인정보처리자인 기관의 리스크: 개요


- 불법행위에 따른 손해배상책임
- 입증책임의 전환
- 징벌적 손해배상책임과 법정 손해배상책임 도입

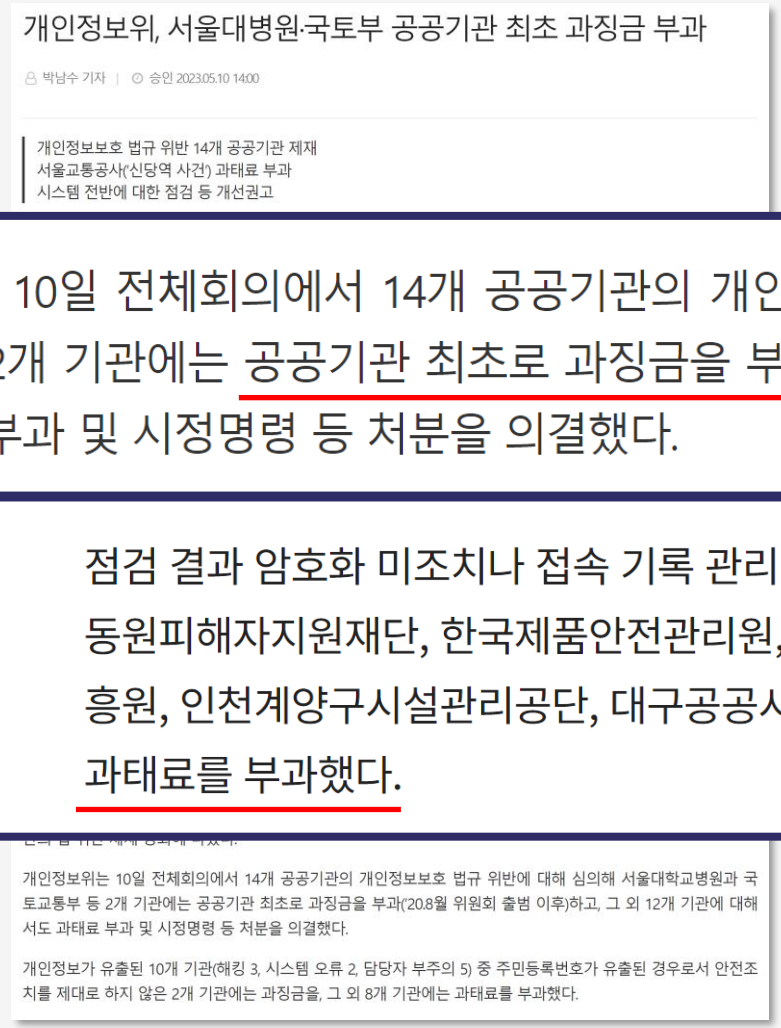
- 위반행위 대부분에 형사처벌 조항 존재
- 양벌규정에 의한 법인 처벌
- 보호위의 형사고발권

- 시정권고, 시정명령
- 과징금, 과태료
- 결과 공표 및 공표 명령 징계권고

# 개인정보처리자인 기관의 리스크: 관련 기관

| | | |
|---|---|---|
| **개인정보 보호위원회** | 공정거래위원회 | 방송통신위원회 |
| 금융위원회/ 금융감독원 | 행정안전부 | 고용노동부 |
| 한국인터넷진흥원 | 경찰/검찰 | 시민단체 |

# 개인정보처리자인 기관의 리스크: 실제 사례



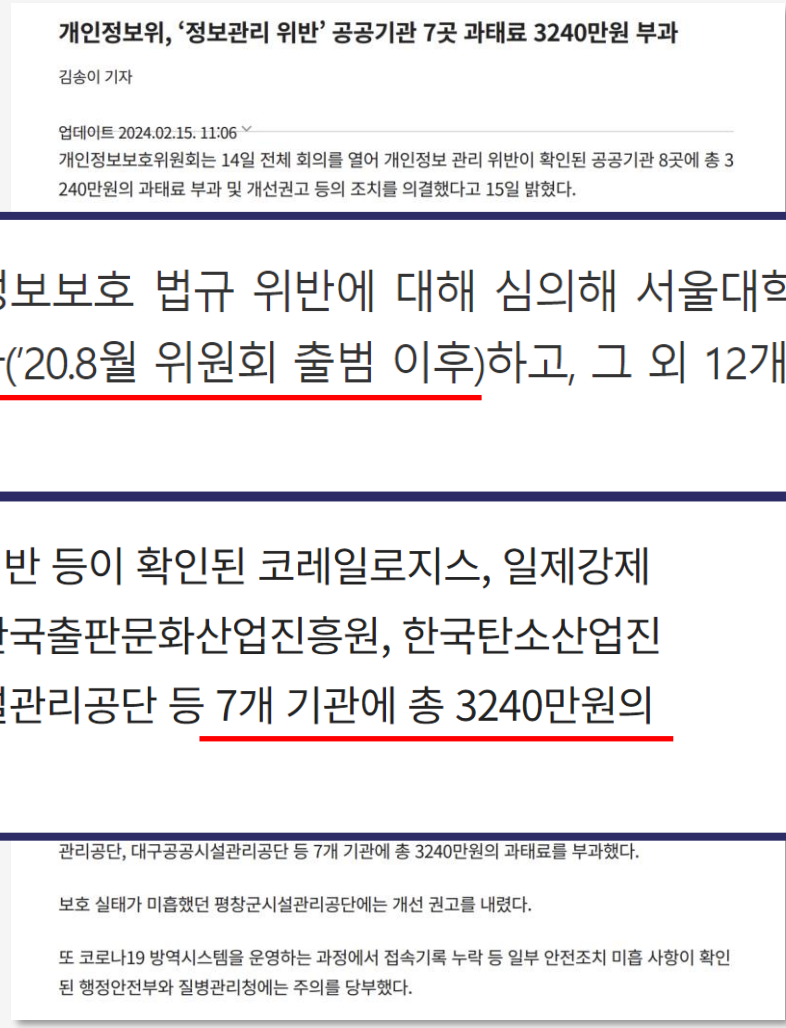
개인정보위, 서울대병원·국토부 공공기관 최초 과징금 부과

박남수 기자 | 승인 2023.05.10 14:00

개인정보보호 법규 위반 14개 공공기관 제재
서울교통공사('신당역 사건') 과태료 부과
시스템 전반에 대한 점검 등 개선권고

개인정보보호위원회는 10일 전체회의에서 14개 공공기관의 개인정보보호 법규 위반에 대해 심의해 서울대학교병원과 국토교통부 등 2개 기관에는 공공기관 최초로 과징금을 부과('20.8월 위원회 출범 이후)하고, 그 외 12개 기관에 대해서도 과태료 부과 및 시정명령 등 처분을 의결했다.

개인정보가 유출된 10개 기관(해킹 3, 시스템 오류 2, 담당자 부주의 5) 중 주민등록번호가 유출된 경우로서 안전조치를 제대로 하지 않은 2개 기관에는 과징금을, 그 외 8개 기관에는 과태료를 부과했다.



**개인정보위, '정보관리 위반' 공공기관 7곳 과태료 3240만원 부과**

김송이 기자

업데이트 2024.02.15. 11:06

개인정보보호위원회는 14일 전체 회의를 열어 개인정보 관리 위반이 확인된 공공기관 8곳에 총 3240만원의 과태료 부과 및 개선권고 등의 조치를 의결했다고 15일 밝혔다.

관리공단, 대구공공시설관리공단 등 7개 기관에 총 3240만원의 과태료를 부과했다.

보호 실태가 미흡했던 평창군시설관리공단에는 개선 권고를 내렸다.

또 코로나19 방역시스템을 운영하는 과정에서 접속기록 누락 등 일부 안전조치 미흡 사항이 확인된 행정안전부와 질병관리청에는 주의를 당부했다.

개인정보위는 10일 전체회의에서 14개 공공기관의 개인정보보호 법규 위반에 대해 심의해 서울대학교병원과 국토교통부 등 2개 기관에는 공공기관 최초로 과징금을 부과('20.8월 위원회 출범 이후)하고, 그 외 12개 기관에 대해서도 과태료 부과 및 시정명령 등 처분을 의결했다.

점검 결과 암호화 미조치나 접속 기록 관리 위반 등이 확인된 코레일로지스, 일제강제동원피해자지원재단, 한국제품안전관리원, 한국출판문화산업진흥원, 한국탄소산업진흥원, 인천계양구시설관리공단, 대구공공시설관리공단 등 7개 기관에 총 3240만원의 과태료를 부과했다.

# 개인정보처리자인 기관의 리스크: 개정법(改定法) 적용 시작

개인정보 유출된 골프존, 과징금 75억원·과태료 540만원 부과 받아

**골프존, 개인정보 유출사고로 과징금 75억원 · 과태료 540만원 · 시정·공표명령**
**기업의 책임성 강화 위해 개정 개인정보보호법 규정 적용 첫 사례**


[이미지=개인정보보호위원회]

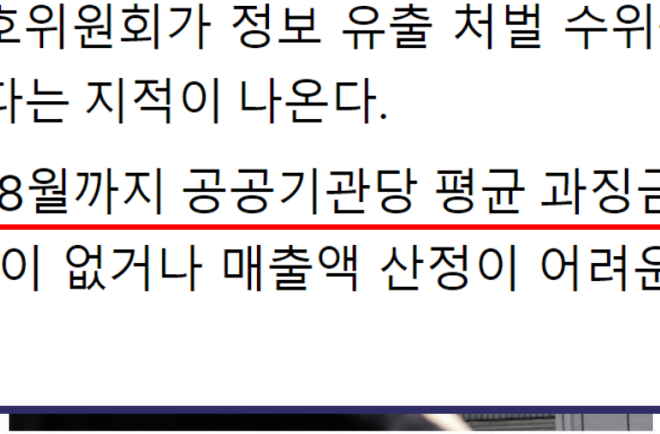
공표명령은 개인정보 보호법 개정(2023년 9월 15일)으로 신설된 처분 규정으로, 사업자 홈페이지 등에 과징금 · 과태료 등의 처분받은 사실을 공표하는 제도다.

골프존은 지난해 11월 해커로부터 랜섬웨어 공격을 받았다. 이 과정에서 해커는 골프존 직원들의 가상사설망 계정정보를 탈취해 업무망 내 파일서버에 원격접속(2023년 11월 22일)하고, 파일서버에 저장된 파일을 외부로 유출(2023년 11월 22일~23일)한 후 다크웹에 공개했다.

**골프존은 75억 부과하고…`개인정보 유출` 공공기관 처벌수위 논란**

김영욱 · 입력 2024. 5. 13. 11:47 · 수정 2024. 5. 13. 13:30

골프존 과징금 75억 부과, 개인정보보호법 개정안 시행 첫 사례



연합뉴스

개인정보보호법 개정안 강화 이후로 개인정보보호위원회가 정보 유출 처벌 수위를 강화하고 있는 가운데 공공기관에 대한 제제도 동반돼야 한다는 지적이 나온다.

작년 9월부터 개인정보보호법 개정안 시행으로 기업의 개인정보 보호 책임이 강화됐다. 지난 8일 골프존이 개인정보 관리 소홀로 221만명의 정보를 유출, 역대 최대인 75억400만원의 과징금 처분이 내려졌다. 개정안 이후 첫 적용 사례다.

개정 전까지 과징금 상한액이 '위법행위와 관련된 매출액의 3%'에서 '전체 매출액의 3%'로 조정, 위반행위와 관련 없는 매출액은 제외하도록 했다. 관련 여부 증명 책임이 기업에게 있어 과징금 부담이 더욱 커졌으며 추후 과징금 규모가 더욱 늘어날 가능성이 존재한다.

개인정보보호법 개정안 강화 이후로 개인정보보호위원회가 정보 유출 처벌 수위를 강화하고 있는 가운데 공공기관에 대한 제제도 동반돼야 한다는 지적이 나온다.

공공기관 유출이 민간의 유출을 넘어섰으나 작년 8월까지 공공기관당 평균 과징금과 과태료는 700만원으로 민간기업의 7%에 불과했다. 매출액이 없거나 매출액 산정이 어려운 공공기관의 과징금은 최대 20억원이기 때문이다.

# 개인정보처리자인 기관의 대응방안

BACK TO BASIC

WHALE & SUN
SPIRIT OF CONSULTATION

# 개인정보 관련 기관의 대응방안 1: Mindset

# 개인정보 관련 기업·기관의 대응방안 1: Mindset

**유의할 법원 판례들**

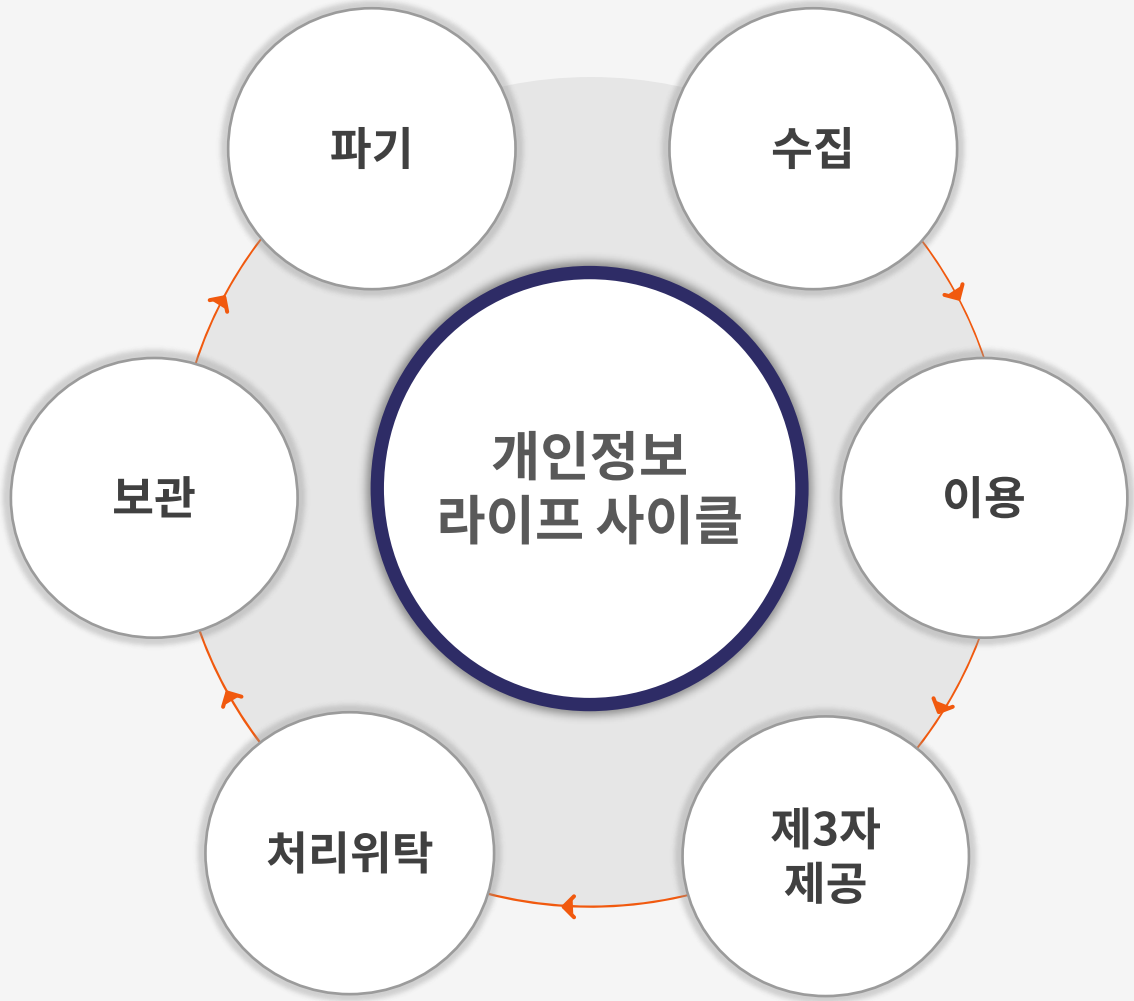
- 고소장에 피고소인의 주소와 전화번호를 기재한 것이 개인정보의 목적 외 이용에 해당한다고 판시한 사례(학과장이 학생회장을 명예훼손죄로 고소한 사건, 서울북부지방법원 2014노202판결, 대법원에서 확정)
- 개인정보의 분실·도난·유출·위조·변조 또는 훼손과 고시 위반행위 사이의 인과관계가 요구되지 않는다고 판시한 사례(인터파크 개인정보 유출 사건, 서울고등법원 2019. 11. 1. 선고 2018누56291 판결)

# 개인정보 관련 기관의 대응방안 1: Mindset

## 개인정보 보호법은 不自然스러운 法이다!

| | | |
|---|---|---|
| 정보 교류라는 인류 생활양식 | VS. | 사생활 보호 |
| 수 만 년 | VS. | 100년 미만 |
| 상식 | VS. | 비상식 |

# 개인정보 관련 기관의 대응방안 2: 처리 현황 점검



# 개인정보 관련 기업·기관의 대응방안 2: 처리 현황 점검

비행기 조종사는 비행 전에 항상 비행기를 철저히 점검한다. 그들은 엔진에 시동을 걸기 전에 비행기의 모든 부분이 제대로 작동하는지 확인하기 위해 세부 사항이 전부 인쇄된 체크리스트를 활용한다. 수십 년 동안 일한 베테랑이라면 이런 점검 과정을 생략하거나 적어도 체크리스트를 쓰지는 않으리라고 생각하는 사람도 있을 것이다. 지금쯤이면 제2의 천성이나 다름없지 않겠는가?

틀렸다. 지금도 모두가 체크리스트를 사용한다. 이들은 근거 없이 낙관하지 않으며, 정밀한 사전 준비를 통해 자신 있게 이륙한다. 승객 또한 조종사의 세심한 준비를 보고 안심할 수 있다.

마이크 벡틀, 내향인만의 무기 중에서

# 개인정보 관련 기관의 대응방안 2: 처리 현황 점검

- **개인정보 보호법 위반 사례 중 수탁자 책임형이 64% 이상**
- **개인정보 유출 사건 중 수탁자 책임형이 77% 이상**
- **사업자의 85%가 시스템 개발 및 운영업무 위탁 중**

IT수탁사 개인정보 처리실태 현장점검 결과 (2014)

- 개인정보 처리 위수탁이란?
- 위탁자의 법적 책임? ① 민사상 손해배상책임(사용자책임), ② 형사상 양벌규정 적용, ③ 행정상 행정제재

# 개인정보 관련 기관의 대응방안 2: 처리 현황 점검

## 나의 처리현황은 물론, 수탁자들도 철저히 점검하고 감독해야!

수탁자에 대한 과징금·과태료 처분 및 형사처벌 규정 신설 ( § 64의2, 71~73, 75)

위탁자의 사용자책임 면책 가능성을 종전과 같이 엄격히 해석하는 것에 대한 비판

- 권영준, "해킹사고에 대한 개인정보처리자의 과실 판단 기준", 저스티스 제132호, 한국법학원, 2012, 65면 등
- 최경진 외 12인, 개인정보보호법, 박영사, 2024, 381면

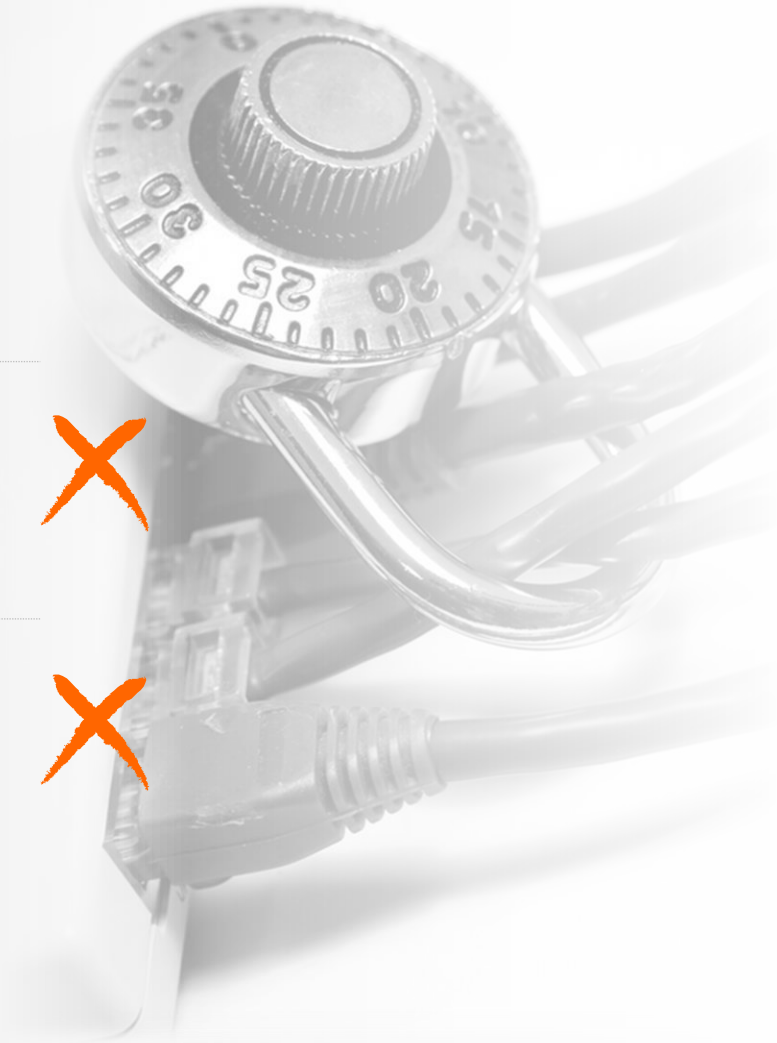
**수탁자의 법 위반 시 위탁자의 민형사 및 행정상 책임이 면책될 가능성 증대**

# 개인정보 관련 기관의 대응방안 3: 법령 준수

“도대체 해킹을 어떻게 막으란 말이냐고!”

“개인정보 보호법은 보안전문가 처벌 전문 법률” ✗

“CISO/CPO를 맡겠다는 사람이 없어서 큰 일 …” ✗



# 개인정보 관련 기관의 대응방안 3: 법령 준수

## 일단 법령이 정한 조치만은 100% 이행한다!

면책을 위한 법령 준수 vs 사건·사고 방지를 위한 법령 준수

법령을 넘어선 기술 발전상에 따른 추가적인 기술적 조치는 선택 사항

보호위도 고시 §6③과 같은 포괄적 규정 해석에 있어서 엄격함과 합리성 갖추어야

# 개인정보 관련 기관의 대응방안 4: 유출 등 사건·사고 대처

"고객 센터·홍보부서부터 총동원하라!"

"Facts Finding! Fact Finding! Fact Finding!"

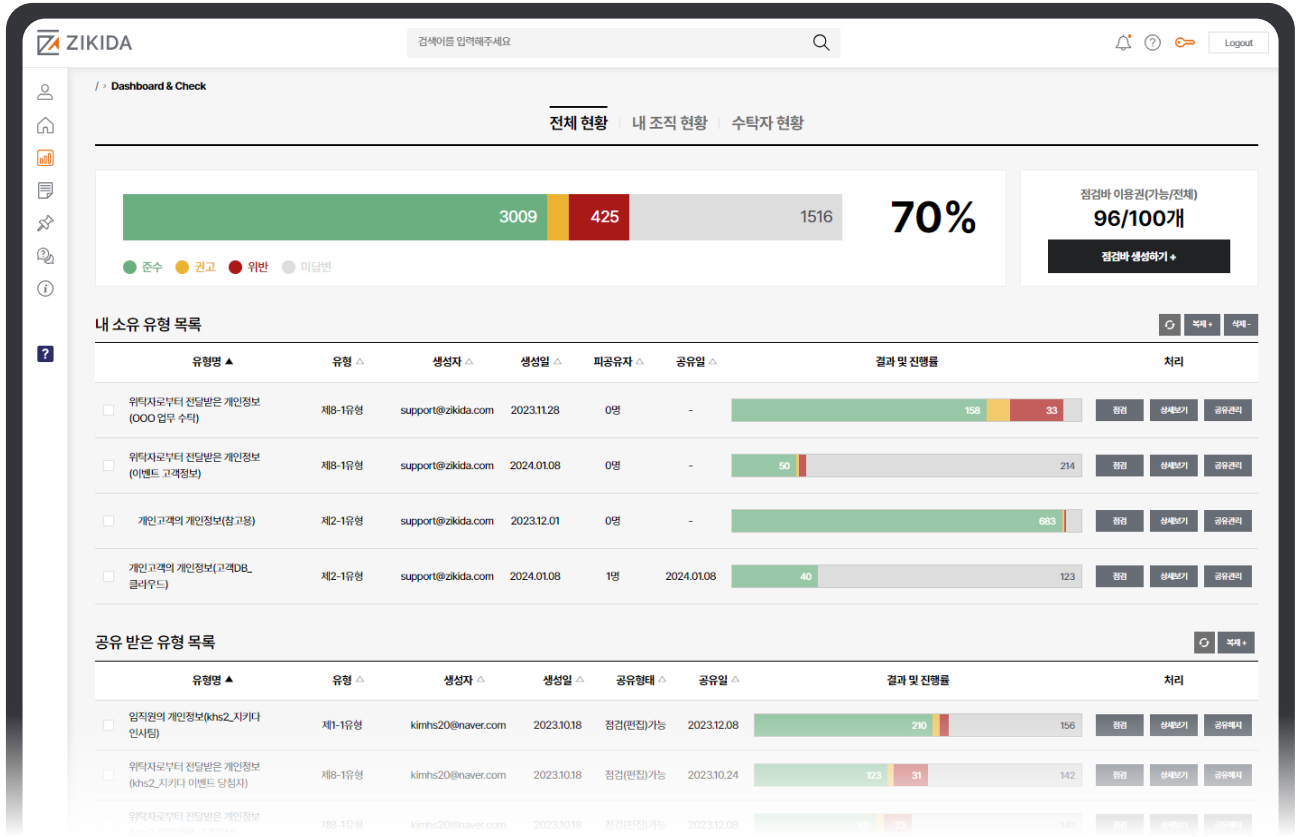
"하늘이 무너져도 솟아날 구멍은 있다... 그것도 항상!"

# Useful Information

ZIKIDA

# 개인정보 관련 '점검'과 '관리·감독' 기능의 완벽한 통합

www.zikida.com




## 개인정보 실태점검 과정과 결과 등의 시각화

점검바(bar)를 통해 기업이나 기관 내·외부를 막론하고,
점검의 전 과정과 결과를 한 눈에 알아볼 수 있도록 지원하며,
그 상태를 실시간으로 모니터링

## 업데이트를 통한 스마트한 관리

법령, 고시, 가이드라인, 해설서, 행정해석, 판례 등을 반영하고
그 변동에 따라 지속적 업데이트를 진행하여 편의성 뿐만 아니라
기업이나 기관의 리소스(resources)를 크게 절약

## 기업 내부 및 수탁자에 대한 지속적 관리·감독 수행

법 위반 또는 best practice에 따른 권고 사항 등을 정확히 타겟팅
하여 기업 내부 및 수탁자들에 대한 실질적인 관리·감독 달성

# Any Question?

변호사 김진환

kim.jh@whaleandsun.com / kim.jh@zikida.com

02-592-0153 / 010-9337-0741