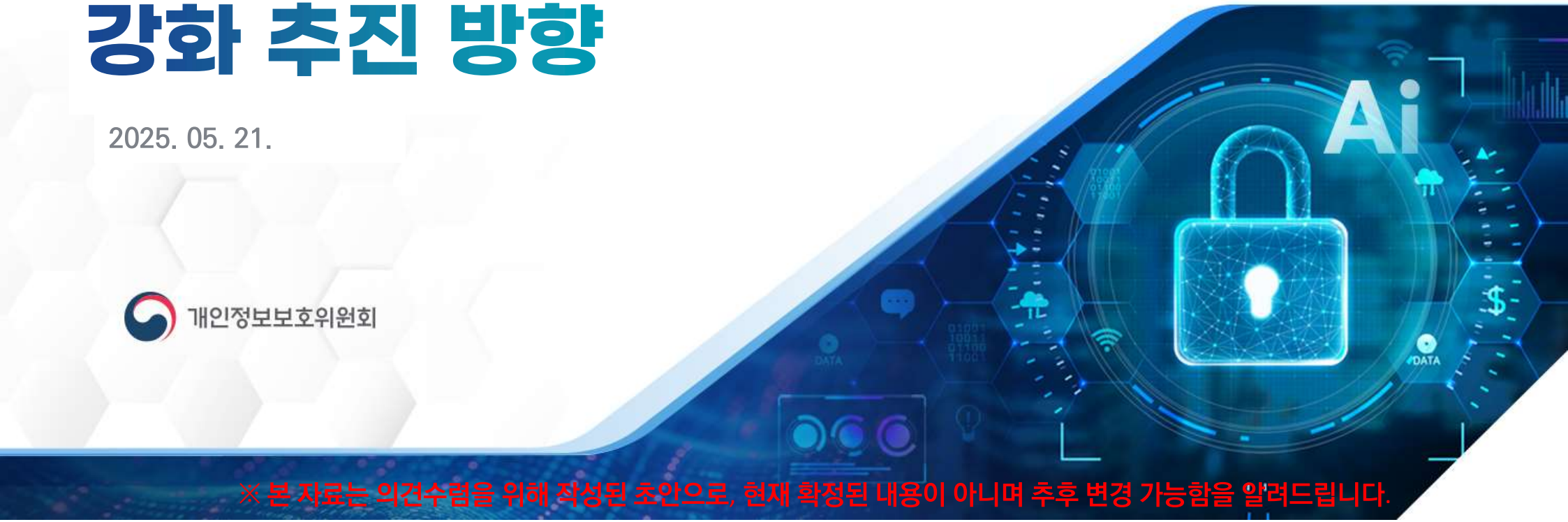
‘SKT 대규모 개인정보 유출’ 계기
개인정보 안전관리 체계 강화 추진 방향

2025. 05. 21.

개인정보보호위원회



※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

개인정보보호위원회

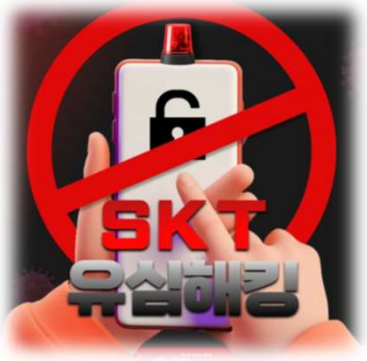
Ⅰ. 추진 배경

Ⅱ. 핵심 추진방향

Ⅲ. 추진 과제

① 즉각적 · 기술적 조치사항 강구
② 상시적 · 전사적 내부통제 강화
③ 정보주체의 권리구제 효율화

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.



SKT 고객정보 유출사고는 인공지능 심화 시대의 핵심 기반인 신뢰 인프라를 훼손하는 "중대한 사건"

- 최근 유출 사고는 개인정보 처리가 수반되는 모든 산업분야의 안전성에 대한 국민적 불안감 유발
- AI, 자율주행 등 신기술 발전으로 예측 불가능한 보안 위협 및 개인정보 침해 요인이 진화 중이나
  - 국내 기업들은 AI 심화 시대에 필요한 성숙한 개인정보 위험관리 체계가 미비한 경우가 다수

→ 유사 사례의 재발 방지를 위해 제도적·기술적 문제점 진단 및 보완 필요
이를 위해 종합적 "개인정보 안전관리 체계 강화 대책" 수립·시행 추진

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

핵심 추진방향

시급성, 중요성을 고려한 **종합적 안전관리 대책** + CPO 중심의 전사적 내부통제 강화를 위한 **정책적·제도적 지원** + 정보주체 (유출피해자) 중심의 **실질적 피해구제 체계**

개인정보 처리가 수반되는 **全산업분야 · 全주기**에 걸친 **총체적 점검·보완**

개인정보 보호 = '비용'→ **'전략적 투자', '기본적 책무'**라는 사회적 인식 확립

국민의 신뢰를 받는 개인정보 안전관리체계 조성

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

핵심 추진방향

» 개인정보를 다수 처리하고 대국민 영향도가 큰 **대규모 개인정보처리자**(예: 100만명 이상) **중심으로 적용** 추진

유사사고 예방을 위한 ① 즉각적 · 기술적 조치사항

- 개인정보 전 주기에 걸친 점검 및 이상탐지
- 암호화 적용 확대 및 관리 강화
- 다크웹 유통정보 분석을 통한 2차 피해 예방
- ISMS-P 실효성 강화

② 상시적 · 전사적 내부통제 강화

- 개인정보보호 분야 투자 (인력, 예산) 최소기준 명확화
- CEO/CPO 중심의 내부통제 강화
- 개인정보 영향평가 활성화
- 개인정보 기술분석센터 신설 및 내부통제 기술지원 강화

③ 정보주체의 권리구제 실질화

〈현행 제도는 실질적 피해구제에 한계가 있어 발표내용 외 다양한 의견을 수렴하여 종합 검토 중〉

- 피해회복과 과징금 감면 연계 및 집단분쟁조정 실질화
- 시장감시, 권리구제 지원 등을 위한 개인정보 옴부즈만 설치

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

추진과제 : ① 즉각적 · 기술적 조치사항(1)

» 개인정보 전 주기에 걸친 점검 및 이상 탐지

취약점 제거

개인정보처리시스템 대상 외부인 시각의 모의해킹 실시, 취약점 점검 및 보완 정례화

+

이상 징후 탐지

접속기록 등 자동화된 분석을 통한 이상징후 탐지* 적용 확대

* '개인정보의 안전성 확보조치 기준' 제17조에 따라 공공기관을 대상으로만 접속기록 자동분석 시행 중('24.9.15~)

» 암호화 적용 확대 및 관리 강화

- 법정 의무 암호화 대상 외 개인정보*에도 암호화 적용을 한 경우 유출 시 과징금 감경 등 인센티브 제공

  * 결합키로 사용 가능한 정보(전화번호 등), 이름, 상세주소 등

  암호화 외에도 모의해킹 등 자발적 · 선제적 보호조치시 과징금 · 과태료 부과 등에 전향적 고려 가능

- 유출시에도 복호화할 수 없도록 암호키는 별도 분리보관, 비밀번호는 솔트값*을 추가하여 안전도 향상

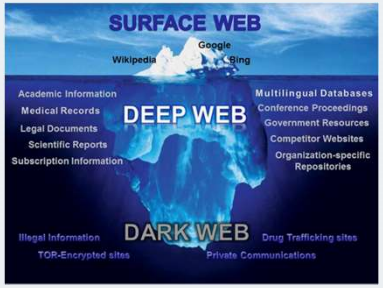
  * 비밀번호에 임의의 값을 추가하여 원래 정보를 쉽게 추정하거나 찾을 수 없도록 하는 방법

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

추진과제 : ① 즉각적 · 기술적 조치사항(2)

» 다크웹 유통 정보 분석을 통한 2차 피해 예방 강화

• 다크웹상의 불법유통 개인정보에 대한 조기경보 체계 구축



개인정보 탐지시 해당 **개인정보처리자 및 유관기관에 신속 공유**
정보주체 **유출통지, 유출경로 확인 및 차단조치** 등 지원

※ '25년 관계기관 협업 하에 모니터링 운영 → '26년 전용 예산확보 및 조기경보 체계 구축

» ISMS-P 실효성 강화

심사 실효성 제고	사후관리 강화	ISMS-P 의무화 검토
• 인증기준 강화(인력구성 등) • 취약점 점검, 모의해킹 실시	• 유출사고 발생시 긴급 점검 • 중대결함 발견시 인증취소	• 개인정보 처리 규모, 중요 기반시설 해당 여부 등 고려

과기정통부 합동

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

추진과제 : ② 상시적 · 전사적 내부통제 강화(1)

» 개인정보 보호 분야 투자(인력, 예산) 최소기준 명확화

* (기존) 사업성, 경제성 논리에 밀려 개인정보 보호 분야 투자 미흡 → (개선) 인력, 예산의 구체적 기준 마련

인력기준 (가안)

- 최소 1명 이상 개인정보 보호 전담인력 배치(CPO 제외)
  ※ 강화된 안전조치가 적용되는 공공시스템은 시스템별 전담인력 확보
- 전체 IT인력의 최소 10% 개인정보 보호 담당인력 배정
  (정보보호 업무 병행 가능)

+

예산기준 (가안)

- '27년까지는 전체 IT예산의 최소 10% → '30년까지는 15%로 확대 (정보보호 예산 포함)

※ 이상행위탐지 시스템, 취약점 점검, 모의해킹 등 투자 필요 분야에 반영

전문 CPO 지정 의무기관 대상 권고

① 매출액 1,500억원 이상 & 100만명 이상 개인정보(또는 5만명 이상 민감 · 고유식별정보) 보유 개인정보처리자

② 상급 종합병원 ← 현재 별도기준 없음

③ 공공시스템 운영기관 ← 현재 기관별 1명 전담인력 배치

미국 기업 IT예산 중 정보보호 투자 비율은 10.5% ('21~'23, 3년간), 국내 기업은 6.1%에 불과

※ '23 Security Budget Report(IANS/Artico) , 정보보호 공시 현황 분석 보고(KISA),

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

추진과제 : ② 상시적 · 전사적 내부통제 강화(2)

» CEO/CPO 중심의 전사적 내부통제 강화

* (기존) CPO 권한 · 위상 부족으로 내부통제 미흡 → (개선) CPO의 실질적 권한 강화

CEO 책임강화
- 최종 책임자로서 노력의무
- CPO가 CEO · 이사회에 보고

CPO 지정신고제 도입
- CPO 지정시 개인정보위 신고 의무화
- 직위 요건(임원의 범위 등) 명확화

CPO 직무여건 보장
- 임명 및 해임절차, 임기보장 등을 통한 CPO의 안정적 직무수행

» 개인정보 영향평가 활성화

* (기존) 공공기관에 한해 일회성 영향평가 → (개선) 민간에서도 자율적 · 체계적으로 수행할 수 있는 여건 조성

외부 평가기관 중심 평가 › 기관 책임하에 수행 (평가결과 경영진 보고 등 CPO 역할 강화)

+

공공기관에 한해 영향평가 의무화 › 민간의 자율적 영향평가 활성화 (민간은 자체평가 허용)

※ 영향평가는 대규모 개인정보처리시스템을 신규 구축하거나 변경하는 경우에 위험 요인을 사전 분석하고 개선하기 위한 평가

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

추진과제 : ② 상시적 · 전사적 내부통제 강화(3)

» 개인정보 기술분석센터 신설 및 내부통제 기술지원 강화

* (기존) 복잡화, 전문화되는 기술환경 대응 어려움 → (개선) 사고분석, 대책공유, 기술지원 등을 위한 전담 · 조직인력 신설

역할	기술 역량을 바탕으로 취약점 분석, 사고분석, 대책 공유 등 기술적 지원 역할을 수행
기대효과	실환경을 모사한 테스트베드를 통해 취약점 분석 결과를 내부통제에 반영하여 개선

» 대규모 수탁자, 솔루션 제공자에 대한 관리감독 강화

* (기존) 중소상공인 개인정보 관리역량 취약 → (개선) 다수 기업이 이용하는 대규모 수탁자, 솔루션 제공자 관리체계 강화

관리감독 효율화

- 보호법상 개선권고 대상 확대 검토 (수탁사, 솔루션 개발/공급자 등)
- 대규모 수탁사 관리체계 개선 검토 (위탁기관별 점검→ 전문기관 검검)

솔루션 인증제 도입

- 개인정보 처리 수반 솔루션(H/W, S/W)에 대한 PbD 인증체계 도입 추진

※ EMR, 셀러툴, 웹호스팅 등 특정분야의 개인정보처리 솔루션의 최소 안전기준 설정

중소영세사업자 지원

- 개인정보 관련 법령 · 기술 컨설팅, 보안솔루션 도입 비용 지원 등 실시

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

추진과제 : ③ 정보주체의 권리구제 실질화

» 피해회복과 과징금 감면 연계 및 집단분쟁조정 실질화

* (기존) 기존 제재만으로는 피해구제 한계 → (개선) 과징금 감면 등과 연계하여 사업자의 자발적 피해구제 유도

- 현행 제재수단(과징금, 과태료 등)은 실질적 피해구제에 한계 → 피해보상 등을 통해 구체적 피해회복시 과징금 감면과 연계

- 보험 약관에 분쟁조정 합의금이 누락되어 있어 가입자 혼란 → 분쟁조정 합의금을 손해배상 보험 약관에 명문화
- 사업자의 자발적 대책 마련 요구 등 적극 조정

» 시장감시, 권리구제 지원 등을 위한 '개인정보 옴부즈만' 설치

* (기존) 정보주체의 목소리를 청취할 수 있는 창구 부재 → (개선) 정보주체가 참여할 수 있는 개인정보 옴부즈만 설치

※ '옴부즈만'은 공공기관이 책무를 적절히 수행하는지 여부를 국민을 대신하여 감시하고자 선출된 대리인을 말함

- 〈구성〉 15인 이내로 학계, 시민단체 및 일반국민(공개모집) 중심으로 구성
- 〈운영〉 반기별 1회 회의 개최, 옴부즈만에서 논의 안건을 제시하면 개인정보위는 검토 후 의견 제시(필요시 조사 및 개선권고 등)

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

본 발표 자료는
현 시점에서 검토 중인
최소한의 대책(안)으로
향후 수정 · 보완 될 수 있음

앞으로도 각계 각층의 다양한 의견을
수렴하여 6월 중 확정할 계획임

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.

감사합니다

개인정보 안전관리 체계 강화 추진방향

개인정보보호위원회

※ 본 자료는 의견수렴을 위해 작성된 초안으로, 현재 확정된 내용이 아니며 추후 변경 가능함을 알려드립니다.