비상경제본부 회의 겸
경제관계장관회의 겸
국가창업시대 전략회의
26-15-3
(공개)

예방 중심
개인정보 관리체계 전환 계획

2026. 5. 22.

관 계 부 처 합 동

예방 중심 개인정보 관리체계 전환 계획(요약)

◇ **AI·플랫폼 경제 확산, 클라우드 기반 정보처리 확대 등 데이터 처리 환경이 복잡해지면서 보호조치 대상, 유출 위험 요인도 증가**

◇ **AI 활용 공격 현실화 등 사고 발생 개연성도 높아져 사고를 온전히 막기 어렵고*, 2차 피해에 더해 사회적 비용까지 유발(예: 피싱범죄)**

* 특정 업종에 국한되지 않고 온라인 플랫폼을 활용하는 서비스업 전반으로 공격 확산

◇ **사고 피해를 최소화하고 사회 전반의 보호수준을 제고하기 위해 위험을 사전에 식별 및 관리·대응하는 예방·관리 체계로 전환 추진**

* **'예방 중심 개인정보 관리체계 전환 계획' 국무회의 보고**('26.5.12.)
☞ (대통령 지시사항) "**공공부문 개인정보 보호 실태**를 **지속 점검**할 것", "**개인정보·데이터 관리 전담 인력 확보**를 위해 기존 인력 재배치를 우선 검토하고, **필요 시 인력을 증원**할 것"

1 위험 기반 예방관리체계 운영

□ **(위험 기반 실태점검)** 산업분야, 개인정보 처리양태·특성 등을 고려해 고·중·저 위험군을 분류하고, **위험에 비례하는 차등적 관리·점검**

○ **(고위험군 : 정기·수시 점검)** 위원회가 **점검분야** 사전 **공개 후 점검**, **미흡사항**은 **시정권고**하고 **이행여부**를 **일정 기간**(예: 2년) **지속 관리**

- **CPO 중심 내부통제** 실태를 **중점 점검·관리**하여 **사고 위험 최소화**

- 현황 분석을 통해 **기초 위험지도 구축, 점검대상 선정**에 활용('26~)

• 【고위험】 100만명 이상 개인정보, 고유식별정보·민감정보 처리
→ PbD 원칙, ISMS-P 인증, 영향평가, 보호활동 공개, CEO 책임경영 등 준수 유도
※ '26년 점검 대상 : 플랫폼, 금융기관(은행, 보험, 카드 등), 공공기관, 에듀테크, 요양병원

○ **(중위험군 : 자체+합동 점검)** **부처**가 **소관 분야 실태점검** 실시, 개인정보위와 점검 결과 검토 및 이슈 발생 시 **합동 점검 추진**

• 【중위험】 처리규모, 유형 등 상대적으로 위험 수준이 낮으나 부처의 체계적 점검·관리가 필요한 분야
→ 공공기관 보호수준평가, (자체)영향평가, PbD원칙 준수
※ 산업별 특성을 반영한 점검항목을 개인정보위와 합동 개발·점검, 점검결과 공유·관리
※ **산업 분야별 평가·인증**(예, 호텔업 평가 등)기준에 개인정보 보호 항목을 추가 반영하여 기본 수준 확보

○ **(저위험군 : 자율점검)** **자율 점검도구**를 **지원**하되, 필요시 개인정보위와 부처 **합동점검을 통해 기본 보호수준 확보**

• 【저위험】 1만명 이하 개인정보, 단독으로 개인 식별이 어려워 피해 영향이 낮은 정보 처리
→ 자율규제단체와 협업 등으로 자율점검, 안전조치 현황 점검 및 컨설팅 등 준수 지원

○ **(신기술 점검)** 침해 우려사항 점검 및 정책 환류(예: IoT 기기, 에이전트 AI)

□ **(안전조치 기준 개정)** **위험 분석 기반**의 안전조치 중·장기 개정방향을 마련하고, **개인정보 처리 흐름, 유형 등을 고려**한 **보호기준으로 개정**

※ ('26) 보호기준 개정방향 마련, ('27) 선택사항으로 일부 적용, ('28) 전면 개정 추진

□ **(범부처 협력체계 구축)** 주요 산업 분야 중심 **정책협의체 운영**(수시)

○ 부처별 **소관분야 개인정보처리자** 대상 **지속 점검·지원**, 부처의 개인정보 보호 활동에 대한 현황 확인 및 **미흡요인 해소 지원**

○ **공공 AX 혁신지원 헬프데스크, 위협 조기경보 연락체계*** 등 운영 협력

* 국내외 서비스·기술, 사고 동향을 파악하여 CPO협의회 등 협·단체와 핫라인을 통해 위협 정보 전파·공유하고, 평가·인증의 중점 점검항목에 수시 반영

2 자발적 보호투자 조기 확대 유도

□ **(PbD 원칙 내재화)** 서비스 기획·설계·개발 단계부터 개인정보 보호를 기본으로 하는 **개인정보 보호 중심 설계 원칙**을 **법제화**('26~)

○ **(원칙 안착유도) 안내서·우수사례** 보급*, **평가·인증 기준****에 반영 등 ('27~)

* **처리단계별 개인정보 최소화**, 보유기간 경과시 **파기 대신 익명화** 조치 등 개인정보 생애주기별 위험 감소조치의 구체적 방안을 안내서로 개발

** 기획단계 CPO 검토 및 의견반영, 설계단계 PbD 적용 등을 ISMS-P, 개인정보 영향평가에 반영

○ **(PbD 인증제 확산) 시범대상을 중소기업 활용솔루션**까지 확대, 법적 근거 마련 추진('26~)

□ **(인센티브 재설계)** 위험 감소를 위한 **투자노력시 과징금 감경** 등 체계 정비,

* 보호 관련 인력·예산 외 **지속적 보호활동 실행 결과** 등으로 투자노력 확인시 감경

- **중소·영세사업자**의 **경미한 법 위반**은 **기술지원** 등을 통한 **시정** 시 **처분을 경감**하도록 시행령 등을 개정하여 **실질적 보호투자 유도**

< 참고: 전주기 보호를 위한 추가 보호조치(예시) >

설계: PbD	운영: Zero-trust	대응·회복
•**(Privacy by Default)** 보호 기본값 설정 •**(영향평가)** 추가적 PIA 수행·지속 관리 •**(다크패턴 방지)** 공정한 UI/UX, 본질적 통제권 보장 등	•**(접근통제)** RBAC 기반 최소권한 부여, 데이터 단위 접근통제 •**(인증)** 추가적 MFA, FIDO 기반 인증, 지속적 인증·검증 •**(데이터 보호)** 추가적 암호화, 대규모 다운로드 통제 등	•**(모의훈련(해킹))** 취약점 신고·조치·공개(CVD/VDP) •**(외부점검)** 보안진단, 인증 등 •**(지속 점검)** 상황기반 이상행위 분석 및 차단 •**(훈련)** 위기상황 대응 훈련

※ 추가적 보호조치에 대한 정책 표명 외 실질적 운영 사실을 입증할 수 있는 명확한 근거 필요

□ **(책임경영 강화)** CEO·CPO 활동을 포함한 보호활동을 **ESG 평가** 지표로 반영하고, **'정보보호 공시*'**에 개인정보 보호 활동 포함 유도

* (現 **공시항목**) 투자, 인력, 인증·평가·점검, **보호활동 현황**(정책, 사고대응체계, 인식제고 등)
※ 보호활동(예시) : 영향평가, PbD 검토 등 추가조치 내역, CPO 점검결과, 이사회 보고현황 등

○ CPO 대신 **전문가가 점검·조치 지원**하는 소상공인용 **구독형 컨설팅** 추진

○ **공공부문 보호수준 평가 내실화** 및 **인력·재원 확충, 전담공무원 육성**

* 개인정보 보호 직무에 대한 수당 등 처우 개선 추진

• 【공공부문 현황조사 결과('26.2.)】 전담인력 수요는 기관당 3.2명(現 전담인력은 0.7명)

3 개인정보 보호 생태계 활성화

□ **(공급망 관리)** 대량의 개인정보가 집중되는 **SaaS·전문수탁자** 등에 대한 **고강도 점검·조치로 보호조치 공백 방지**

○ **클라우드·플랫폼** 특성에 맞게 **PbD 원칙 준수**사항을 **가이드**로 개발('26~)

* **(예 : 클라우드)** 사업자 간 **책임 범위 명확화**(공급망 책임추적성), **설정 오류 탐지·관리**, 개인정보 **접근경로 식별,** 파기 결과 확인, **API 생애주기 점검·관리 등**

□ **(예방 · 보호 기술)** AI 학습시 침해위협을 방지하는 **예방형 PET*** **연구개발**

* AI 환경에서 유출·불법유통, 오남용 등 차단기술 등 R&D 로드맵 마련·개발('26년~)

□ **(중소기업 지원)** 선제적 안전조치 컨설팅, 유출사고시 피해복구 지원 등 **중소사업자 보호수준 향상** 유도

□ **(전문인력 양성)** 권역·지역별 **전문인력**(석·박사급)**을 양성**하고, 직무·역할 맞춤형 현장**실무 교육 프로그램**도 **설계·운영**

* 우아한형제들 등 민간기업의 개발자 교육에도 개인정보 보호 반영 추진

4 국민이 체감하는 신뢰문화 조성

□ **(정보주체 생애주기 교육)** **아동·청소년** 및 **디지털 취약계층** 대상 **교육** 추진

* 권리행사 역량이 취약한 아동·청소년 개인정보 보호를 위한 법제 개선도 추진

□ **(안심환경 조성)** 생활분야 처리방침 **집중점검,** 다크패턴 등 **신뢰 저해 관행 개선**

□ **(국민 참여 · 체감형 프로그램)** **범국가적 보호 캠페인, 보호 실천 홍보활동*** 확대

* ATM기기 보호수칙 안내, 지하철·역사 내 홍보, 공문하단 개인정보 보호 슬로건 게시 등

☞ **"개인정보 보호가 기본이 되는 안심 사회 (Privacy by Default)" 구현**

순 서

Ⅰ. 추진배경

□ **데이터 경제 전환**으로 **개인정보 활용 규모·범위**가 **구조적으로 확대**

○ AI 서비스 확대, 플랫폼 중심 경제 확산, 클라우드 기반 서비스와 정보처리 확대* 등으로 인해 **개인정보 처리 규모·환경도 크게 변화 중**

* 전세계 데이터 규모 : '25년 180ZB → '30년 612ZB (1ZB=1조GB, 영화 400억편 분량)

○ 데이터 처리 환경이 복잡해지면서 개인정보 처리도 **다수 시스템이 관여**하게 됨에 따라 **보호조치 대상, 유출 위험 요인**도 함께 증가

※ **(과거) 정형데이터**, 처리 **흐름 명확**, 개별 의무 중심 **경계 보호·시스템 보호** → **(현재) 비정형데이터** 확산, 처리 **흐름 불명확**, 전방위적 **상시 보호·데이터 보호**

□ 그럼에도 **기업의 대응**은 기존 환경에 안주하는 사이에 유출사고는 **피해 규모, 빈도, 대상 모두 증가·다변화되는** 추세

○ 해킹 대상이 특정업종에 국한되지 않고 **온라인 플랫폼**을 활용하는 **서비스 전반**으로 **확산**, 기술·관리·외주 등 **복합원인으로 사고발생**

< 최근 5년간 개인정보 유출사고 현황 >

▪ **(신고건수)** '20년 219건 → '25년 447건 (2배↑), **(유출규모)** '20년 12,003천건 → '25년 103,546천건 (8.6배↑)

▪ **(유출분야) 정보·통신**(28%), **유통·물류**(20%), 제조(10%), 보건·복지(8%), 기타(16%) 등 *의결건수기준

○ 피해는 **유출**에 그치지 않고 **보이스 피싱** 등 정보주체에 대한 2차 피해뿐만 아니라 **사회적 비용**까지 유발(예: 통신사 유심교체 등)

□ 처리자를 **관리·감독**의 대상으로 보는 **엄벌 중심**의 보호체계와 더불어 처리자와 **함께** 보호 환경을 조성하는 **예방 관리 강화** 추진

☞ **"개인정보 보호가 기본이 되는 안심 사회 (Privacy by Default)" 구현**

※ 위험요인 사전진단·예방관리는 사고피해 최소화, 신속 원인파악·대응 등 대응력도 제고 효과

Ⅱ. 현황 및 문제점

1. (보호체계) 획일적 규율은 위험 대비에 한계

□ 사후 대응 중심의 관리 구조

○ 현행 개인정보 보호 법체계는 조사, 시정명령, 과징금·과태료 등 **사후 집행수단은 비교적 강력**하게 개편하였으나,

○ **ISMS-P***, **안전성 확보조치, 영향평가** 등 예방적 수단은 실질적 이행과 입증 보다는 최소한의 기준만 충족하는 **형식적 이행** 우려도 있음

* 인증 이후에는 인증기준을 제대로 유지하지 않아 유출사고가 발생하는 사례 발생

□ 위험 기반 차등 규율의 미흡

○ 업종, 처리규모 등을 고려하지 않은 **일률적 제도 적용***으로 인해 최소 기준에 수렴하는 **하향 평준화된 규제 준수**를 초래하면서

- **처리자 간**(고위험분야, 영세사업자 등) **법적 준수 이행 괴리**도 **발생****

* (예) 안전성 확보조치는 모든 처리자에게 공통 부과되는 일반 규정

** 고위험 분야는 강화된 보호투자가 필요하나 법적요건 충족에 안주하여 실질적 조치를 최소화, 영세사업자는 과잉 규제에 따른 비용 부담으로 이행을 포기하는 양극화 발생

○ 최근 유출사고는 제조·의료·교육 등 **전 분야에서 빈번히 발생**하나, 분야별로 **상이한 위험 구조, 보호 수준**을 반영한 정책 추진체계 미흡

※ 산업·기술별 특성 등을 고려하지 않은 **범용기준은 보호조치 등 준비·유인에 한계**가 있고, AI 에이전트, 프로파일링 등 심각한 미래 위험에 효과적 대응 불가

□ 단일 처리자, 행위 유형 중심 규율체계

○ 현행 법체계는 **개별 처리자** 중심으로, 수집·이용·제3자 제공·위탁·파기 등 **개별 행위유형 단위로 규율**하는 구조

○ 이는 복잡한 공급망 구조 속 **실효적 통제** 및 **예방 관리에 한계***

* 수탁사·개발사, 클라우드, 플랫폼사 등 다수 사업자 관여 환경에서 책임 소재·범위 불명확, 대규모 결합, 비정형데이터 활용 등 새로운 위험은 행위유형만으로는 규율 곤란

2. [투자체계] 자율적 · 능동적 예방 활동에 대한 유인 부족

□ '보호를 잘하는 조직'에 대한 **포상** 또는 **과징금 감경 제도 미비**로 **자발적**으로 개선 대책을 찾을 **유인이 부족**하며 **소극적 대응 초래***

* 유출사고 발생시 유출 신고를 하지 않거나, 사고 관련 자료를 조직적으로 폐기

□ CPO 지정 의무가 법률에 규정되어 있으나, 조직 내 **개인정보 보호의 책임성 및 지속성**을 **담보**하는 **제도적 장치**는 **미흡**

○ 일부 대기업을 제외하면 CPO의 독립성, 정기 보고, 내부 감사, 재발방지 점검 등 내부 관리 체계가 제도화되어 있지 않은 실정

○ **중소기업**은 전문인력, 예산 부족으로 인해 보호체계 구축 여력이 제한적이며, 개인정보 보호 투자가 **최소 법 준수 수준**에 머무르는 경향

○ **공공부문**은 대량의 개인정보를 포함한 행정정보를 처리함에도, 전담인력 확보, 상시 취약점 점검 등 **예방 중심 내부 역량 확충 미흡***

* 최신 보안패치 적용은 **7%**, 보안 취약점 전수점검 비율은 **17%**에 불과
(공공분야 개인정보처리시스템 387개 대상 긴급 실태점검 결과, '26)

※ 전체 IT예산 대비 정보보호 예산 비중은 **9.9%**, 개인정보보호 분야 '26년~'27년 필요 예산 총액은 2,035억원(653개 공공기관 예산현황 전수조사 결과, '26)

□ 해외 주요국*도 **설계·운영** 단계에서 '**책임성**(Accountability)' 및 '**지속적 위험 관리**(Resilience)'를 강화하는 추세

* Privacy Framework(NIST, 미국), Digital Security Risk Management(OECD) 등

[참고] 미국 국립표준기술연구소(NIST)의 Privacy Framework

- **(개요)** 조직의 프라이버시 위험 이해, 평가, 우선순위 설정, 소통을 돕는 자율적 도구
- **(주요내용)** 조직이 달성해야 할 프라이버시 위험관리 목표 및 활동을 5개 항목을 중심으로 평가·계획할 수 있도록 제시 (Identify, Govern, Control, Communicate, Protect)

3. (보호생태계) ICT 생태계 변화에 대응할 산업 기반 미흡

□ 클라우드, AI 제공자, 솔루션 개발사 등 **다수 주체**가 **관여**하는 **복합적인 공급망** 속 구조적·입체적 대처가 필요하나, **처리자 중심 대응체계**로는 **한계**

○ 사고 책임은 공급망 전체가 아닌 '**일선 처리자**'**에게 전가**되는 구조로, **설계 단계부터 보안을 고려**하는(PbD) 협력적 보호체계 **미흡**

□ AX 전환 가속화로 **미래 위험 대비 필요성**은 커지고 있으나, 개인정보 보호 강화기술(PETs) 연구·개발(R&D) 및 **실증 확산 기반 미비**

○ 개인정보 보호 R&D는 정보보호 분야 대비 **기술개발 투자 미흡**

* 개인정보 보호 R&D 규모는 '26년 132억원으로 정보보호(1,191억) 대비 11% 수준

○ 동형암호, 합성데이터 등 PET에 대한 정책적 논의는 활발하나*, 개별 기업이 독자적으로 도입할 수 있는 **업종별 표준 모델** 및 **실증사례 부족**

* 예: OECD AI보고서(2025), NIST의 Privacy Enhancing Cryptography 프로젝트 등

□ 현장의 수요에 비해 **전문인력 수급** 및 **실무 기술 인재 양성기반 취약**

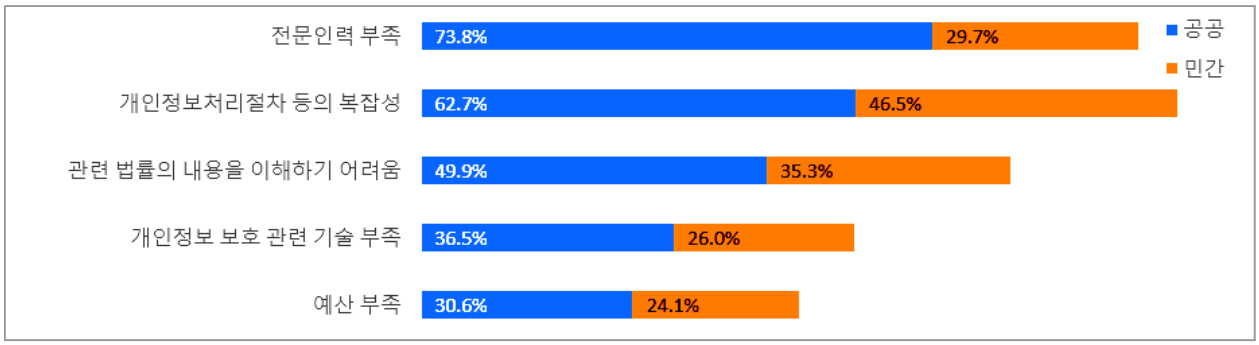
○ 법·관리적 지식과 기술적 실무 능력을 겸비해야 하는 융합형 전문가* 수요는 급증, 이를 공급할 **전문교육 프로그램**은 **부족**

* 예: 단순 정보보안 지식 뿐만 아니라 AI 모델의 편향성 제거, 데이터 비식별화 기술 적용 등 고도화된 실무 지식 필요

○ CPPG* 등 기존 자격제도는 법 준수 및 관리체계 점검에 집중하여, **보호조치를 직접 설계·구현**할 **기술 인력** 양성 기반 전무

* 개인정보관리사(CPPG): (사)한국CPO포럼이 발급하는 국내 민간 개인정보보호 전문 자격증

< 개인정보보호 업무 관련 애로사항('22) >



4. (국민인식) 개인정보 신뢰 문화 부재

□ 사회 전반의 개인정보 보호 수준은 규제·기술 뿐만 아니라 개인정보 처리자·취급자, 정보주체 등 **모든 참여주체의 인식과 행동**이 좌우

○ 개인정보 보호 중요성에 대한 **국민의 높은 인식 수준***에 비해, **경영 전반의 문화**와 **일상적 실천**으로 내재화되지는 못한 상황

* '개인정보 보호의 중요성'에 대해 처리자는 85% 이상, 정보주체는 92% 이상이 중요하다고 응답

※ 개인정보취급자 교육을 실시하는 민간기업은 8.8%, 개인정보 처리 동의 시 내용을 확인하는 정보주체 비율은 55.4%에 불과 (2024 개인정보보호 및 활용조사)

□ **생애주기별·역할별** 특성에 맞는 **교육 프로그램, 내용 등 인프라**가 **미흡**하여, 현장에서는 교육이 구체적 실천으로 연결되지 못함

○ 초·중·고, 공공·민간 임직원 및 취급자 등 연령·역할·산업분야 등에 특화된 신뢰 문화 조성 **교육프로그램 미흡**

○ 전문교육은 **형식적 이수**에 그치거나, 법 준수와 관리체계 운영 등 일부에 치우쳐 있어, **실제사고 대응**이나 설계 과정부터 **보호조치 반영 등 현장 역량 강화로 이어지지 못**하는 한계

□ 보호 규정은 있으나, 사회 전반의 **신뢰 경험**이 **축적**되지 못하는 구조

○ 일부 서비스에서는 과도한 개인정보 수집, 형식적 동의, 다크패턴 등 **불합리한 개인정보 처리 관행**이 지속되고 있어, 서비스 이용을 위한 동의 등 **권리 행사 과정**에서 국민의 **피로감 누적**

○ 반복된 유출사고로 개인정보 보호에 대한 **정보주체의 효능감도 저하**

* "거의 매달 정보유출 사고...'더 털릴 것도 없다' 허탈" (국민일보, '25.12.1)
"'안일함에 더 분노', '너무 털려 이제는 체념'... 속 끓는 소비자들"(연합뉴스TV, '25.12.7)

< 왜 지금 사전 예방 관리를 강화하는가? >

□ **AI·플랫폼·클라우드 확산**으로 개인정보 처리 위험의 **규모·복잡성**이 **증대**되고, 기존 제도로 포착·통제하기 어려운 **새로운 프라이버시 위험영역**(gray area) 확대

□ 사후 대응 위주의 법·제도만으로는 기술 변화에 따른 위험 확산 속도를 따라잡기 어렵고, 피해 **예방·회복**에도 **한계**

□ **안전한 활용**, **지속가능한 혁신**의 전제 조건인 개인정보 보호 기반 확보를 위해 **설계·운영단계**에서의 **책임성 및 위험기반 예방 관리** 강화 필요

	As-Is		To-Be
보호 체계	**획일적 · 일률적 규제** 적용	▶	**위험 기반 차등적 점검·관리**
예방 투자	**최소 규정 준수** **하향 평준화**된 보호 **투자** **책임성 담보** 장치 **미흡**		법정 조치 외 **추가적 안전조치** 유도 위험 기반 **능동적·자발적 예방 투자** CEO·CPO 중심 보호**책임 강화**
보호생태계	신기술 R&D, 실증 기반 미비 복합 공급망 대응 한계 체계적 인력양성 기반 미흡		**신기술 대응 역량 강화** **산업 생태계 경쟁력 제고** **전문인력 양성** 기반 구축
인식 · 문화	대상별·역할별 교육 미흡 정보주체 신뢰 훼손		**맞춤형 교육 활성화** 개인정보 **신뢰문화 조성**

Ⅲ. 추진 전략

비전 ‘개인정보 보호가 기본이 되는 안심 사회’ 구현

4대 전략

❶ 위험 기반(Risk-based) 예방 관리체계 구축 · 운영
❷ 자발적 보안 · 보호 투자 조기 확대 유도
❸ 예방적 개인정보 보호 기술 · 산업 생태계 활성화
❹ 국민이 안심하는 신뢰 문화 조성

4대 전략	주요 추진과제
1 위험 기반 예방관리체계 구축·운영	1 위험 기반 실태점검체계 정착 2 예방적 보호제도 개선 3 범부처·민관 공동 협력 보호체계 구축
2 자발적 보안·보호 투자 조기 확대 유도	4 인센티브 재설계로 능동적 보호투자 유도 5 CEO·CPO 중심 책임경영 강화
3 개인정보 보호 생태계 활성화	6 보안·보호기술 산업 경쟁력 제고 7 전문인력 양성 기반 구축 8 신기술 대응 · 감독 역량 강화
4 국민이 안심하는 신뢰 문화 조성	9 대상별 맞춤형 교육 확대 10 안심할 수 있는 서비스 환경 조성

Ⅳ. 주요 추진과제

전략 1. 위험 기반(Risk-based) 예방관리체계 구축·운영

〈 기 본 방 향 〉

◈ 사후 제재 중심에서 **위험 기반**(Risk-Based)**의 예방 관리 체계를 강화**하여 **산업 전 분야**에서 촘촘하게 **기본적인 보호 수준 제고**

◈ 예방 취지에 맞게, **처분을 전제로 한 조사와**는 **엄격히 분리** 운영

◈ **부처 및 민관 협업**을 통해 **위험 요소 신속 파악** 및 **선제적 대응**

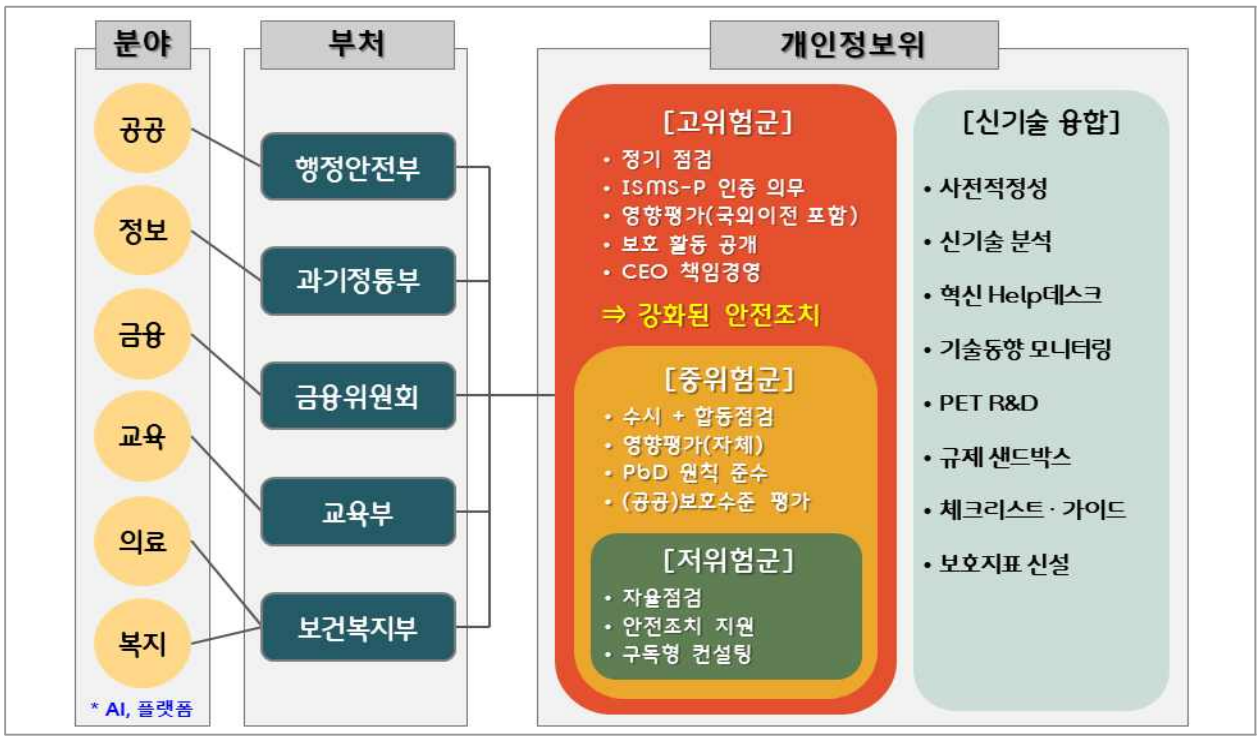
1 위험에 비례하는 다층적 점검체계 정착

□ **(기본방향) 위험 수준** 등에 따라 실태점검, ISMS-P 인증, 개인정보 영향평가, 강화된 안전조치(모의해킹 적용등) **관리수준 적용 차등화**

○ 실태점검은 원칙적으로 **조사 절차와 엄격히 분리·운영**하고, **개선이 필요한 사항은 시정권고**하여 **조치 유도**

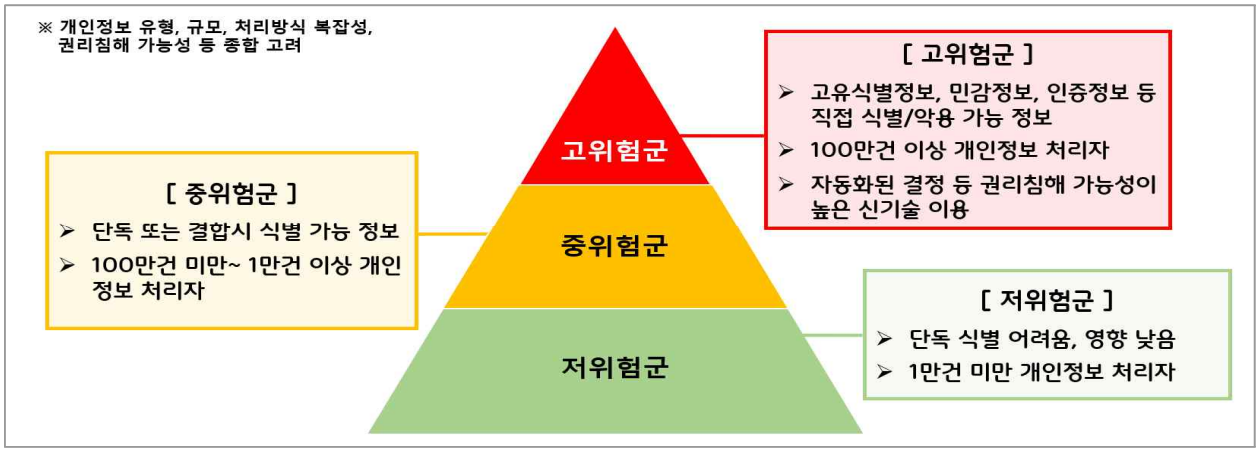
※ 제재를 전제로 한 조사와 달리 과징금·과태료 부과 등 단계가 없음(☞참고 1)

[위험기반(Risk-Based) 예방 보호 체계]



□ **(위험 기반 실태점검)** 산업분야, 개인정보 처리양태·특성 등을 고려해 고·중·저 위험군을 분류하고, 위험에 비례하는 **차등적 관리·점검**

[개인정보 유형별 위험기반(Risk-Base) 분류 체계(안)]



○ **(고위험군 : 정기·수시 점검)** 개인정보위는 점검분야 사전 공개 후 실태점검, **미흡사항**은 **시정권고**하여 **이행여부**를 **일정 기간**(예: 2년) **지속 추적 관리**

- **대규모·고위험 처리자*** 등은 CPO 중심의 **내부 통제** 실태를 **중점 점검, 정밀관리**하여 **사고 위험 최소화**

* 통신/금융/보건·복지 등 100만명 이상, 신기술 분야, 권리침해 가능성 등 종합 고려

※ **(점검항목)** 서비스 설계·변경시 CPO의 검토 내역, 권한 검토·조정 내역 등 증빙

< 2026년도 개인정보 고위험군 4대 분야 실태점검 대상(안) >

분야	정보통신	금융	공공	복지
대상	플랫폼	은행, 보험사, 카드사, 증권사	공공기관	요양병원
집중점검	대규모 데이터 처리	고유식별정보 처리	취약점 점검	민감정보 처리
관련 부처	과기정통부	금융위	전부처	복지부

※ 추진과정에서 변경될 수 있음

< 고위험군 실태점검 절차(안) >

점검대상 선정	➡	자료요구 및 현장점검	➡	쟁점파악 등 결과분석	➡	관련부처 협의	➡	시정권고 등 후속조치
1/4분기		2/4분기		3/4분기		3/4분기		4/4분기

* 소관부처의 연례 점검 외에 개인정보위도 주기적·집중 점검하여 상호 보완

○ **(중위험군 : 자체+합동 점검) 각 부처**가 **소관 분야**에 대해 **자체 실태점검** 실시, 개인정보위는 실적 관리 및 이슈 발생 시 **합동 점검 추진**

* (합동점검 사례) 항공 분야 개인정보취급자 접근통제 실태 점검(국토부), 공교육 플랫폼의 개인정보 관리실태 점검(교육부) 등

** 합동점검 근거: 개인정보보호법 제63조의2(사전실태점검) 제6항

- 부처의 중점 점검 요청사항에 대해 개인정보위가 부처와 함께 맞춤형 실태점검 후 개인정보처리자에게 개선사항 **조치 유도**

< 중위험군 합동점검 절차(안) >

부처 요청 대상 선정	➡	자료요구 및 현장점검	➡	쟁점파악 등 결과분석	➡	관련부처 협의·통보	➡	개선사항 등 후속조치
소관부처 개인정보위		개인정보위 소관부처		개인정보위		개인정보위 소관부처		개인정보위 소관부처

○ **(저위험군 : 자율점검)** 상대적으로 위험도가 낮은 분야는 **자율 점검도구 지원***, 필요시(사회적 이슈 발생 등) **합동점검으로 기본 보호수준 확보**

* 업종·기술 특성이 반영된 분야별 체크리스트 개발·배포('26~'27)

※ 보호법상 의무 전반(안전조치, 동의, 파기 등)을 점검할 수 있는 점검도구를 지원하고, 필요시 부처에서 법 준수 여부를 확인·관리하는데 증적으로 활용

- 산업별 개인정보 보호 **자율규제 단체를 단계적으로 확대**, 자율규약을 제정·체결하여 **단체별 자율보호 활동** 후 개인정보위에 **결과 보고**

※ 산업별 평가지표와 연계, 우수 사업자 포상 확대 등 인센티브 다각화

□ **(신기술 이슈점검)** 음성·영상 등 개인정보 처리가 수반되는 신기술·신서비스 분야는 개인정보 침해 **우려사항** 등을 **점검하여 정책으로 환류**

※ '26년도 결과는 분야별 가이드라인 마련 및 제도 개선을 위한 정책으로 환류

< '26년 점검대상 및 내용(안) >

분야	점검대상	점검내용
IoT	카메라 영상 기반 IoT 기기 (예: 스마트홈, 웨어러블 등)	기기·서버 내 개인정보 저장, 국외 전송, 암호화 여부, 기기 내 개인정보 처리 구조 등 점검
AI	Agentic AI 개발 프레임워크 (예:LangChain, CrewAI(Google) 등)	과도한 개인정보 수집·이용, 외부 전송, 로그기록 등에 개인정보 포함 등 점검

※ 대상은 세부 실태점검 계획 수립 시 변경될 수 있음

□ **(사회적 이슈점검)** 대규모·고위험군에서 개인정보 침해·유출사고 발생 시 원인 분석 후 **유사 분야 집중 점검하**여 동종 **유사업계**의 **재발방지** 주력

※ '26년도는 대량의 민감·중요정보가 포함된 상조·금융·고객상담센터 등 분야 점검 실시

□ **(기초 위험지도 구축)** 개인정보 처리 규모·항목, 관리실태 등 **현황** 분석을 통해 **기초 위험지도**를 **구축***하고, **점검대상 선정 등**에 활용

* 전문가·CPO 등으로 연구반 구성 및 조사 항목, 문항, 조사 대상 등 검토·마련

※ 현황 조사 방안 마련('26.), 기초 위험지도 구축·조사(~'27)

2 예방적 보호 제도 개선

□ **(ISMS-P 개선)** 공공시스템운영기관, 이동통신사업자, 본인확인기관 등 대규모 개인정보를 처리하는 **공공·민간**의 **주요 처리자** 대상 **의무화**('27)

○ 매출액·처리 규모 등을 고려하여 의무화 대상을 '27.7월부터 단계적 확대

* 공공시스템 : 100만명 이상, 취급자 200명 이상, 주민시스템과 연계 등 387개 지정 (시행령 §30의2)

◈ **ISMS-P 인증**: 신청기관의 정보보호 또는 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 제도 (망법 §47, 보호법 §32의2)

현 행		개 선
· 범용적인 인증 기준, 연1회 스냅샷식 심사 구조로 신기술 위험 대응 미흡	▶	· 위험기반 차등 인증, 현장실증·사후 점검 강화로 상시관리형 심사 전환

○ **(인증기준 개선)** 주요 **보안위협 사례, 주요국 보안 요구** 사항 등을 **참조**하여 강화된 **인증 기준 마련*** 및 인증기준 **안내서 개정**('26~)

* **강화인증**을 **신설**하여 인증을 3단계로 구분(간편-표준-**강화인증**신설)하고, 강화인증 **대상**에 대해서는 자동화 도구를 활용한 정보자산 식별 강화, 무결성 검증 등 **강화기준 도입**

○ **(심사품질 강화)** 인증심사 투입 **인력·기간 확대**, 인증심사 **절차 개편*** 등 **현장실증 점검** 강화 및 **스냅샷** 방식의 심사 **한계 극복****('26~)

* **예비심사**에서 핵심항목 **미충족** 시, **본심사 불가** 및 **기술심사 도입**하여 부실심사 사전차단

** **보안 관리체계 지속·적정** 운영 여부를 사후심사 시 **집중 점검** 등 **자체 상시 점검체계** 확립

□ **(안전조치 기준 개정)** 위험분석 기반의 안전조치 중·장기 개정방향을 마련하고, 개인정보 처리흐름·유형 등을 고려한 **보호기준으로 개정**

◈ **안전성 확보조치**: 개인정보의 안전성 확보에 필요한 기술적·관리적·물리적 안전조치에 관한 최소한의 기준을 규정하고, 처리자는 스스로의 환경에 맞는 필요한 조치 적용

현 행	▶	개 선
· 사고 사례 대응 중심의 부분·수시 개정		· 위험분석 기반 체계로 종합 개편

○ 획일적인 기준 적용이 아닌, **위험분석을 기반**으로 처리자 스스로 안전조치 적용 여부 및 **적용 수준을 달리** 할 수 있도록 개선*

* 예: 암호화, 개인정보처리시스템에 대한 접근제한 조치 등 차등 적용

※ ('26) 보호기준 개정방향 마련, ('27) 선택사항으로 일부 적용, ('28) 전면 개정 추진

□ **(영향평가 실질화)** 처리흐름, 위험 식별·조치보다 법 준수에 초점을 맞춰 진행되는 **영향평가 제도를 PbD 원칙과 연계**하여 기준 등 개선*

※ 개인정보위의 평가 결과 검토 및 의견제시 절차에 대한 실효성 확보 방안도 마련

◈ **개인정보 영향평가**: 개인정보 처리로 인한 잠재적인 개인정보 침해 발생 가능성 및 영향을 사전에 조사·예측·검토하여 개선방안을 도출하는 체계적인 절차 (보호법 §33)

현 행	▶	개 선
· 법 준수 확인 위주의 평가 관행 고착화, 평가 품질 정체로 실질적 위험평가 한계		· PbD 원칙과 연계하여 사전예방 기능 강화

○ **(방법 구체화) 민간** 영향평가의 실행력 제고를 위해 **평가 대상 및 방법 등*** **구체화**('26~), 추진단계별·위험수준에 따른 평가방법 차등화('27~)

* GDPR 등 해외 영향평가 사례 분석, 기존 공공기관 대상 영향평가 문제점 진단 등을 바탕으로 영향평가 실효성 강화를 위한 대상·방법·기준 개선방향 도출

○ **(국외이전 영향평가) '국외이전 영향평가제'**를 **신설***('27)하여 **대규모·민감정보**의 이전, **보호수준**이 **우려**되는 **국가로**의 이전에 대한 **보호조치 강화**

* 이전되는 국가의 개인정보 보호 법제, 정보주체의 권리 보호 절차 등을 고려하여 국외이전 시 위험성을 자체적으로 평가·보관토록 규정, 체크리스트 등 사업자용 도구 개발·제공

○ **(평가 품질 관리)** 공공기관 영향평가 관련, 평가결과 **등록 여부 점검** 및 평가결과물 **샘플링 심층점검** 등을 통해 평가 품질 향상 도모('26)

3 범부처 · 민관 공동 협력 보호체계 구축

□ **(범부처 협력체계 구축)** 전 산업 분야에서 개인정보 활용이 확대됨에 따라 안전한 개인정보 활용·관리를 지원하는 **범부처 협력체계 구축**

○ **(정책협의체 운영)** 범부처 정책협의체를 구성, 부처의 소관 산업분야 관리실태 점검 현황 파악, 위험 해소방안 등 협력(수시)

- 협의체 논의를 통해 소관분야 개인정보처리자 대상 지속 점검·지원, 부처의 개인정보 보호 활동에 대한 현황 확인 및 미흡요인 해소 지원

< 정책협의체 논의 과제(안) >

• **분야별 실태점검 및 개선조치 현황**	• 자율규제 활동 지원
• 소관 분야 위협 동향 공유·전파	• 분야별 제도 개선 사항 협의
• 평가·인증 내 보호지표 신설·강화	• AX 지원 등 정책 추진과정의 보호 협력

○ **(범정부 보안점검)** 대규모 해킹 공격 대비 를 통해 유출·침해 사고 발생 전 대응에 **자원 투입 강화**과기정통부, 국정원 협업

- 공공부문 주요 개인정보처리시스템 대상 **모의해킹 의무** 등 보호조치 강화

○ **(신사업지원)** AX 전환 사업 등 신사업 추진시 개인정보 안전조치 방안 등 컨설팅, 분야별 부처 합동점검 등을 지원하는 체계 마련('26~)

※ **공공 AX 혁신지원**, **사전적정성 제도** 등을 활용하고, KISA에 협력지원팀 구성·운영

- **(공공 AX 혁신지원)** 신뢰 기반의 **범정부 인공지능 전환(AX) 확산**을 위해 의료·복지·납세 등 **국민 생활과 밀접한 데이터**를 **프라이버시 리스크 없이 안전하게 활용**할 수 있도록 **맞춤형 지원**('26~)

< 「공공 AX 혁신지원 헬프데스크」 개요 >

대상	▸AI 신서비스 기획 단계에서 개인정보 보호법 저촉 여부가 불확실한 정부부처·공공기관 - ①기관 신청 또는 ②타 기관 공공 AX 과제 중 프라이버시 이슈 예상 사업 선제 발굴·지원
지원 방안	▸기관별 서비스 구조, 개인정보 처리 흐름, 프라이버시 리스크 요인 분석을 토대로, ▲적극적 법령해석, ▲원스톱 가명처리, ▲사전적정성 검토, ▲샌드박스(규제 특례) 등 연계

※ 과기정통부 IRIS(범부처통합연구지원시스템) AI 고도화 관련 사전적정성 검토(3.11. 의결)

- **부처·기관**이 공공 AX 추진시 **기획·설계 단계**부터 스스로 리스크를 식별하고 경감방안을 적용할 수 있도록 AX 프라이버시 점검도구 제공('26~)

□ **(민관 예방협의체 운영)** 위협 요소를 사전에 발견하고 피해를 최소화하기 위한 개인정보 위협 **조기경보 연락체계**(EWS)*를 구축·운영

< 개인정보 침해·유출 사고 라이프 사이클 >

구분	사고 예방 단계	사고 발생 단계	사고 사후관리 단계
목적	**사고 방지**	사고 감지·대응, 확산 방지	피해복구, 재발방지
활동	• **EWS 운영, 모니터링** • **보안 정책 수립·이행** • **교육, 취약점 점검 등**	• 이상징후 탐지·차단 • 긴급 대응 • 영향 파악, 신고·통지	• 정보주체 피해 지원 • 사고 원인 분석·개선 • 재발방지대책 수립·이행

○ **(위협 정보 전파)** 개인정보 관련 국내·외 **서비스·기술 동향,** 침해·유출 등 **사고 동향(원인·기법) 등** 위협 트렌드를 **신속하게 전파**하여 민관이 즉시 **대응**할 수 있도록 **지원**(상시)

※ CPO협의회 등 협·단체와 위협정보를 전파·공유하는 핫라인을 운영하고, 자체 점검을 통해 유사사고에 대한 사전 대응 및 조치 유도

○ **(위협 정보 점검)** 확인된 위협 트렌드의 중요도를 고려하여 **ISMS-P 인증, 개인정보 보호수준 평가 등의 중점 점검항목**에 추가 **반영**(상시)

※ 개인정보보호 담당자의 유출 사고대응, 안전조치 가이드에도 활용

전략 2. 자발적 보안·보호 투자 조기 확대 유도

〈 기 본 방 향 〉

◈ 인센티브 재설계를 통해 법적 최소기준 준수를 넘어 PbD 원칙을 반영하고 **기업의 능동적 투자 유도**

◈ CEO·CPO 중심으로 개인정보 **보호 책임경영 환경 조성**

1 인센티브 재설계로 능동적 보호투자 유도

□ **(PbD 원칙 내재화)** 서비스 기획·설계·개발 단계부터 개인정보 보호를 기본으로 하는 **개인정보 보호 중심 설계 원칙**을 **법제화**('26~)

※ **Privacy by Design and by Default** : 제품 또는 서비스의 기획, 제조, 폐기 등 전 과정에서 개인정보 보호 요소를 충분히 고려함으로써 개인정보 침해를 사전에 예방하는 설계 개념

※ **개정방향(안, §3)** '사생활 침해 최소화'를 '기본값 보호'로 확장하고(제6항), 서비스·시스템 기획 단계의 개인정보 보호 원칙에 따른 설계 의무 신설(제9항)

※ 보호법 제29조에 따른 안전조치 기준에 PbD 원칙 반영도 검토

보호법 제3조(개인정보 보호 원칙)
⑥ 개인정보처리자는 정보주체의 권리와 자유를 보호하는 방식으로 개인정보를 처리하여야 하며, 정보주체의 별도 설정이 없는 한 서비스 제공에 필수적인 개인정보 외 개인정보가 수집, 처리되거나 제3자에게 제공되지 아니하도록 기본 설정을 구현하여야 한다.
⑨ 개인정보처리자는 개인정보 처리와 관련된 서비스·시스템의 기획 단계에서 개인정보 보호 원칙에 부합하도록 설계하고 운영하여야 한다.

○ **(원칙 적용지원)** 기획·설계시 참조 **안내서·점검도구·우수사례** 보급, 개인정보 관련 평가·인증 기준*에 반영 등 **PbD 안착 유도**('27~)

* CPO 기획단계 검토 및 의견반영, 설계 단계에서 PbD 적용 등을 ISMS-P, 개인정보 영향평가에 반영

※ **처리단계별 개인정보 최소화**, 보유기간 경과시 **파기 대신 익명화** 조치 등 개인정보 생애주기별 위험 감소조치의 구체적 방안을 안내서로 개발

○ **(기본설정 점검)** 웹·앱 **기본설정**이 PbD 원칙에 부합*하는지 **점검·개선**('26)

* 선택동의, AI 학습에 활용 등은 '동의 비활성화'를 기본설정으로 하였는지 점검·개선

○ **(PbD 인증제 도입·확산)** PbD 인증제 시범대상을 **중소기업 활용 솔루션***까지 확대 및 인증제 **법적 근거 마련 추진**('26~)

* 근태관리 솔루션(안면인식), 보안솔루션(암호화 등), 셀러툴 등 개인정보 처리 자동화 도구

□ **(인센티브 개편)** 사고 발생시 형식적 보호 노력에 따른 제재 감경이 아닌, 실효적 **보호수준 확보시 제재 완화**를 통해 **예방 투자 유도**

○ **(과징금 재설계)** 설계부터 사고대응까지 **위험 감소를 위한 투자노력시,** 인센티브 부여 등 **보호투자**에 대한 **과징금 감경체계 정비**('26.9)

* 보호 관련 인력·예산 외 **지속적 보호활동 실행 결과** 등으로 투자노력 확인시 감경

- 전문성 등이 부족한 **중소·영세사업자**의 **경미한 법 위반**은 **기술지원** 등을 통한 **위반행위 시정**으로 **처분을 경감**하도록 **시행령 등을 개정**하여 실질적 보호투자 유도

□ **(실효적 보호, 복원력 확보)** 기업은 개인정보 특성·환경의 위험요인을 사전진단·조치, 사고대응·**피해최소화 등 전주기 보호* 강화**('26~)

* 개인정보 처리 환경 변화 및 사고 위험 속에서 위험 식별, 예방·통제, 탐지·대응, 복구 등 개인정보 보호 수준을 지속 유지·개선

○ **위험분석과 연계**하여 **안전조치 기준**에 최소권한 부여, 지속적 신뢰 검증·제어 등을 추가하고, **과징금 감경시 반영** 추진('26~)

< 참고: 전주기 보호를 위한 추가 보호조치(예시) >

설계 : PbD	운영: Zero-trust	대응·회복
•**(Privacy by Default)** 보호 기본값 설정 •**(영향평가)** 추가적 PIA 수행·지속 관리 •**(다크패턴 방지)** 공정한 UI/UX, 본질적 통제권 보장 등	•**(접근통제)** RBAC 기반 최소권한 부여, 데이터 단위 접근통제 •**(인증)** 추가적 MFA, FIDO 기반 인증, 지속적 인증·검증 •**(데이터 보호)** 추가적 암호화, 대규모 다운로드 통제 등	•**(모의훈련(해킹))** 취약점 신고·조치·공개(CVD/VDP) •**(외부점검)** 보안진단, 인증 등 •**(지속 점검)** 상황기반 이상행위 분석 및 차단 •**(훈련)** 위기상황 대응 훈련

2 CEO · CPO 중심 보호 책임경영 강화 유도

□ **(대기업 책임경영)** ESG평가 등에 지표로 반영 등 **보호 책임경영** 유도

※ 공공기관용 ESG 가이드라인, 민간 ESG 평가자료로 일부 반영 중

○ **(CEO 책임, CPO 역할)** CEO는 보호 인력·예산 지원 등 실효적 관리 의무, CPO는 자원확보 권한 외 주요사항 이사회 보고와 지정신고 의무 부여('26.9.)

< 참고: CEO/CPO 책임 관련 개인정보보호법 규정 >

제30조의3(사업주 또는 대표자의 책임) 개인정보처리자의 **사업주 또는 대표자는** 개인정보의 안전한 처리 및 정보주체의 권리 보호에 대한 **최종적인 책임자**로서 개인정보 보호에 필요한 **전문 인력과 충분한 예산의 지원 등 총괄적인 관리 조치**를 실효성 있게 하여야 한다.

제31조(개인정보 보호책임자의 지정 등) ③ 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 다음 각 호의 사항을 준수하여야 한다.

1. 개인정보 보호책임자를 지정하거나 그 지정을 변경 또는 해제할 때에는 이사회(법인인 경우로 한정한다. 이하 같다)의 의결을 거칠 것
2. 보호위원회에 대통령령으로 정하는 바에 따라 **개인정보 보호책임자 지정·변경 또는 해제에 관한 사항을 신고**할 것

④ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

2. 개인정보 보호에 필요한 **전문 인력의 관리 및 예산의 확보**
3. 사업주 또는 **대표자 및 이사회에** 대한 개인정보 보호 현황 및 **주요 사항의 보고**

○ **(보호활동 공개)** '정보보호 공시'에 **개인정보 보호활동** 포함 유도('27)

* **(정보보호 공시)** 투자, CPO 등 인력, 인증·평가, **보호활동**(정책, 사고대응체계, 인식제고 등)

※ 공개(안) : 추가 보호조치 내역, CPO의 내부통제 점검 결과, 이사회 보고현황 등

※ 안전분야의 KSCI와 유사한 성숙도 평가 모델 도입·공개 방안도 연구·도입 추진

□ **(중소기업 지원)** 법 준수, 사고복구 지원 등 **중소사업자 보호수준 향상 유도**

○ **(구독형 컨설팅) 소상공인** 등 대상으로 CPO 대신 전문가가 점검·조치 및 사고 대응을 지원하는 **구독 컨설팅 서비스** 도입 추진('26~)

* 대상, 방식, **서비스의 CPO 대체 효력** 등 제도화 방안을 우선 연구 후 단계적 확대 검토

※ 방안 연구('26), 서비스 시범운영('27-'28), 제도화('28~)

○ **(기술 지원)** 소기업 등의 **사고시 추가 유출** 및 **피해확산 방지** 대응, **사고후** 내부관리체계 개선, 재발방지 조치 등 **지원체계 확립**('26~)

※ KISA와 사고대응 지원팀 구성·운영 방안 마련·지원 추진

○ **(선제적 안전조치 지원)** 중소사업자* 대상으로 최소한의 안전성 확보조치 마련 여부를 서면·현장진단, 맞춤형 **개선조치 안내**('26~)

* '26년은 60개 중소사업자 대상 시범 수행, 예산확보 후 점검대상·지원범위 확대

□ **(공공부문 역량 확충 및 책임성 강화)** **상시적 보호체계 강화**를 위해 **인적·물적 보강**을 추진하고, 부실 운영에 대한 **책임 구조 강화**

○ **(인력·재원 확충)** **처리 규모·중요도** 등을 고려하여 기관 유형별 개인정보보호 **전담인력*** 및 **재원** 확보 지원**(관계부처협의, '26.上)**

* (공공시스템운영기관) 공공시스템 전담인력 확충, (그 외 기관) 임직원 수, 시스템 수, 개인정보 처리 중요도, 산하·소속기관 수 등 기관 특성에 맞는 인력규모 검토

** 예산 확충 필요 주요 항목 : 취약점 점검, 접속기록 관리, 개인정보보호 솔루션 도입 등

○ **(보호수준평가 내실화)** **유출사고 패널티를 강화**하고 선제적 **예방 지표**를 **신설**하여 사전 예방에 중점을 둔 **개인정보 보호수준 평가 실시**('26)

※ ① 유출 등 사고 시(10점→20점), 처분 시(3점→5점) 감점 확대
② 모의해킹을 포함한 '개인정보 유출 등 사고 예방과 대응 노력' 지표 신설

- '개인정보 보호의 날' 등과 연계하여 **우수기관·직원 포상 추진**

◈ **공공기관 개인정보 보호수준 평가**: 공공기관의 법적 의무사항 이행 수준 및 개인정보 보호를 위한 기관의 노력 등을 중점적으로 평가하여 역량 향상 도모 (보호법 §11의2)

* (평가 대상) 중앙행정기관 및 소속기관, 지자체, 공공기관, 지방공기업 및 교육행정기관 등 1,450여개

○ **(전담공무원 육성)** 개인정보 보호 역량 제고를 위해 관련 직렬·직류 시험에 **개인정보보호 과목 추가*** 또는 관련 과목에 내용 확대 추진

* 현행 5급·7급 공채 정보보호 직류 시험 과목은 정보보호 관리, 네트워크 보안, 소프트웨어 공학, 정보시스템 보안 등 정보보호 일반에 관한 지식 위주로 평가

- 높은 전문성이 요구되는 동시에 사고 책임 부담이 큰 **고위험 업무**로 **기피**되는 **개인정보보호 직무**에 대한 **처우 개선 추진***

* 전문역량 축적 및 장기 재직 유도를 위해 전문교육 확대, 직무수당 지급 등 추진

* 다수부처 공동 직제개정, 전문직 공무원 정원 통합관리 방안 등 개인정보 보호 전담인력 역량 강화 추진

전략 3. 개인정보 보호 생태계 활성화

〈 기 본 방 향 〉

◈ AI 혁신기반인 **보호기술 R&D, 전문인력 양성 등 산업 경쟁력 제고**

◈ 미래 위험에 대비하기 위한 **개인정보위 기술 대응역량 강화**

1 보안 · 보호기술 산업생태계 경쟁력 제고

□ **(공급망 관리)** 대량의 개인정보가 집중되는 **SaaS·전문수탁자** 등에 대한 **고강도 점검** 및 조치를 유도하여 **복합적 공급망** 구조 속 책임 소재 불명확*에 따른 **보호조치 공백 방지**

* 본사·수탁사·협력사, 클라우드·SaaS사업자, 플랫폼·벤더사 등 다수 당사자 간 책임 불명확

○ SaaS·전문수탁자 등 개인정보 처리에 관여하는 공급망 내 다수 사업자에 대한 **점검 및 개선 유도를 위한 법적 근거** 마련('26~)

○ 클라우드·플랫폼 등 분야별 특성에 맞게 PbD 원칙을 준수할 수 있도록 **처리자와 사업자 준수 사항** 등을 가이드로 개발('26~)

* **(예 : 클라우드)** 사업자 간 **책임 범위 명확화**(재수탁자 사전승인·통제 등 공급망 전체의 책임추적성), **설정 오류 탐지·관리**, 개인정보의 **지리적 위치와 접근경로 식별,** 파기 결과 확인, **API 생애주기 점검·관리 등**

○ 전자문서·결재, EMR 등 분야별 전문수탁사, SaaS 사업자, 개발사와 같은 협력업체 등 **점검·관리방안 마련·이행**('26~)

□ **(예방 · 보호 기술)** AI 학습·서비스시 개인정보 침해위협을 방지할 수 있는 **예방형 개인정보 보호 기술(PET*) 연구개발**

* PET(Privacy Enhancing Technology) : 데이터 가명·익명처리, 동형암호, 합성데이터, 분산컴퓨팅 등 개인정보를 보호하면서 데이터 활용을 가능하게 하는 기술

○ **(PETs)** 개인정보 익명처리 고도화 기술, AI 프라이버시 리스크 경감 기술 등 **일상 속 개인정보 보호**를 위한 **기술 개발** 추진('26~'28)

- ‘우수 개인정보 보호 기술의 확산 촉진 및 산업계 상생 협력 강화 등을 위한 ‘가칭’개인정보 보호·활용 기술 대상’ 신설 추진(’26~)

< ’26년 개인정보 보호기술 R&D 현황 >

연번	세부사업명	주요내용
1	**개인정보 안전활용 선도기술 개발**	• 합성데이터, 가명처리, 딥페이크 예방 기술 등 원본데이터 안전활용 기술 개발 • AI 모델 프라이버시 리스크 경감기술 개발
2	**글로벌 개인정보보호 표준 개발**	• 개인정보 표준기술 개발, 국제표준화 추진 • 개인정보 기술 표준화 생태계 구성 및 표준확산 등 사업화 지원
3	**신뢰기반의 AI 개인정보 보호·활용 기술개발**	• 생성형 AI 모델 프라이버시 취약성 평가, 멀티모달형 AI 기반 개인정보 탐지 추적 및 비식별화 기술 개발

○ **(가명정보 활성화)** 가명처리도 **위험도 판단 기준 표준화, 절차·서류 부담 간소화**를 통해 AI 환경에 맞는 효과적인 가명정보 활용 촉진

※ 가명정보 제도: 특정 개인이 식별되지 않도록하여 가명처리하면 동의 없이도 AI 학습 등 과학적 연구 목적으로 데이터를 가치있게 활용할 수 있는 제도

○ **(예방 R&D 기획)** AI 환경에서 유출·불법유통, 오남용 등을 사전 차단하는 **전주기 안심 예방기술*** **등** R&D 로드맵 마련·개발(’26년~)

* (예) 선택적 언러닝 기술, 보이스피싱·딥페이크 2차 피해방지 등 예방형 안전기술 연구 등

< 미래 위협 대비 개인정보 보호 기술 기획(안, 예시) >

위협 요인	대응 기술
다크웹 상 개인정보 불법유통	• 글로벌 다크웹 개인정보 유출 정황 수집·분석 • 서비스/공급 주체 단위 공급망 위험지수 산출 및 대응
Agentic AI 기반 머신러닝 프라이버시 침해	• AI 환경에서 개인정보의 흔적을 제거하는 선택적 머신 언러닝/삭제·폐기 및 증명·검증 기술 개발

□ **(산업별 보호지표 신설)** 의료·여가·제조 등 **산업 분야별 평가·인증제도, 지원사업 등**에 **개인정보 보호 지표** 신설 또는 강화 추진

○ 산업 분야별 특성을 고려한 개인정보 보호 관련 평가·인증 지표를 소관 부처와 협의·마련하고, 분야별로 순차적으로 적용

※ (예시) EMR 인증, 어린이집 인증, 가정용 청소로봇 기준 등

※ 개인정보 보호지표를 추가 반영한 인증에 “개인정보 강화인증 마크(예, +P)” 부여

2 전문인력 양성 기반 구축

□ **(석 · 박사, 인재양성)** 보호·활용 기술 및 법제·경영 등 다학제적 역량을 갖춰 산업 현장의 문제해결이 가능한 **전문인력(석·박사급) 양성**

○ 개인정보 보호 및 안전한 데이터 활용을 위한 예방형 전문인력을 양성하고, 대학 내 **개인정보보호 학과 개설** 및 인재양성 등을 순차적 확대 추진('26~)

○ 개인정보보호학과, 컴퓨터공학과 등에서 활용 가능한 '표준 개인정보보호 교육과정(안)'을 학회 등과 연구·개발('26~)

□ **(직무기반 교육)** 직무, 역할 맞춤형 **실무 교육프로그램 설계·운영**('27~)

< 교육 프로그램(안) >

직 무	교육 대상	교육 내용 예시
정책·관리	CPO, 법무, 정책 담당자	• 개인정보보호법/GDPR/OECD 프레임워크 • 내부통제 설계, 리스크 기반 정책 설계 • ESG+공시+투자 연계방안
운영·점검	실무 담당자, ISMS-P 담당	• 개인정보 처리 흐름 매핑 • 접근통제, 로그관리, 보관/파기체계 • 위/수탁 관리, 점검 대응 및 개선조치
개발·운영	개발자, 보안 엔지니어, AI/데이터 담당	• PbD 설계 방법론 • 제로 트러스트 기반 개인정보 보호 • 데이터 최소화, 가명·익명처리, 암호화 설계 • API/클라우드/AI데이터 보호 구조
리스크·대응	CISO, 보안팀, 사고대응 조직	• 유출 원인·사례 분석 • 사고 대응 프로세스 설계

□ **(자격 제도)** 정보보안 일반과 구분되는 개인정보 보호 분야 전문인재 양성을 위해 '**개인정보보호 공인 민간자격** 또는 국가자격' 제도* 도입

* 개인정보 법·제도 지식, 정보보호·활용 실무 기술, PbD 관점을 겸비한 전문인력 양성 목적

※ 관리체계·법제도 관련 자격 외에 PbD 엔지니어링 전문 자격도 검토(IAPP의 CIPT)

※ (추진일정) 자격 운영방안 마련('26년) → 자격 설계('27~'28년) → 공인 민간자격 지정 또는 국가자격증 신설('29년)

[참고] 개인정보보호 관련 민간자격 운영 현황

‣ 현재 개인정보보호 분야의 공인 민간자격은 '영상정보관리사' 1건 존재, 127개의 등록 민간자격 운영중(''22년 기준, 신규 취득자가 존재하는 자격은 5개)

‣ 개인정보관리사(CPPG), 개인정보취급사(CPPF), 개인정보보호사, 개인정보보호법 교육강사 등

3 신기술 대응 · 감독 역량 강화

□ **(기술분석센터 구축)** 침해 요인의 선제적 해소를 위해 **신기술 기반 제품·서비스**의 **개인정보 처리 방식**을 분석하는 기술분석센터 구축·운영

○ 서비스·제품 등을 직접 설치·운영하면서 **개인정보 처리흐름**과 침해 위협 요인을 **분석**하는 **플랫폼** 개발 및 **전문인력 확충**(~'26.12월)

* AI, IoT 등 신기술 분야별 분석 전문인력 채용(4명, '26)

○ 웹·앱, IoT기기, AI서비스 등 신기술 실증분석으로 **침해위협 요인조치 유도,** 신기술 개인정보 영향분석·기술개발 가이드 등 개발·배포('26~)

< '26년 분야별 세부분석 대상 및 내용 >

Agentic AI	웹·앱	카메라 영상 기반 IoT
과다 수집, 외부 전송, 로그 등에 개인정보 포함 등	행태정보 등 과도한 개인정보 수집 여부	영상·음성 등 개인정보 처리흐름, 암호화 여부 등

○ **중·장기적**으로 **예방형** 보호기술 **R&D 지원,** 중소기업용 **침해위협, 보호기술 성능 등 검증환경**으로 개방·활용 등 발전 도모*('28~)

* 미래 기술이 개인정보에 미칠 영향 분석 등 '기술분석센터 기능 발전방안' 마련(~12월)

※ 발전방안 연구('26), 역할·기능 확대 추진('27~)

[참고] 프랑스 개인정보감독기관(CNIL)의 디지털혁신연구소(LINC)

- **(역할)** 프라이버시 보호기술 동향 모니터링, 기술분석 및 검증, PbD 기술개발 지원 등
- **(주요성과)** IoT기기·블록체인·웹쿠키 등의 데이터 흐름 및 보호 수준 분석, 스마트폰의 데이터 분석, AI 관련 알고리즘 투명성 및 프라이버시 강화 기술 적용방안 마련 등

□ **(디지털포렌식 센터)** **대규모 시스템에서 발생하는 유출**사고 조사 시 **핵심 증거**를 **신속 확보**할 수 있도록 **디지털 포렌식 랩 신규 구축**(~'25)

○ 디지털 증거자료 분석, 증거물 관리를 위한 **전문장비 도입** 등 환경 조성, 전문인력(분석관) 확보 및 기술교육을 통한 **포렌식 역량 강화**('26~)

○ IT 환경 변화에 따라 IoT, 피지컬 AI 등 다양한 시스템의 디지털 증거도 확보할 수 있도록 포렌식 랩 고도화 추진('28~)

전략 4. 국민이 체감하는 신뢰 문화 조성

〈 기 본 방 향 〉

◈ 개인정보 보호를 단순 법 준수나 사후 대응의 문제가 아니라, 국민이 **일상에서 체감**하고 **업무 전 과정에서 실천**하는 **사회적 규범으로 정착**

◈ 기본 소양으로서의 개인정보보호 교육과 사회 전분야 전문교육을 병행

1 대상별 맞춤형 교육 확대

□ **(실무형 교육 강화)** 처리자·책임자·개발자 등 대상별 특성에 맞는 사례 기반, 직무 기반 교육 확대('26~)

○ **(처리자)** 단순 법령 전달식이 아닌 최신 유출·오남용 및 처분 사례, AI 서비스 도입 시 유의사항 등을 중심으로 **사례중심, 현장 교육 확대**

※ [공공] 나라배움터 등 사이버 교육센터 내 교육콘텐츠 배포 및 직원 교육 실시
[민간] '개인정보배움터'(edu.privacy.go.kr)를 통한 온라인 교육 제공중

○ **(책임자)** CPO 대상 교육은 법·제도 뿐만 아니라 내부 통제, 사고 대응, 위험 평가 등 **실무응용** 및 **의사결정 역량 강화** 중심으로 운영*

* 법 준수를 위한 CPO 책임, CPO가 점검해야 할 주요항목, 주요 사고사례, 사고 시나리오별 대응 절차·방안 등 정보공유 방안도 마련·이행

○ **(개발자)** 서비스 기획·설계·개발 시 유의사항 중심으로 교육 컨텐츠 **개발** 및 **민간기업(우아한형제들 등) 개발자 교육에 반영 추진**

- 개발시부터 개인정보 보호가 내재화되도록 PbD 원칙 준수, 시큐어 코딩, 오픈소스 주의사항, 다크패턴 등 UI/UX 주의 사항 등 교육

※ (예비 창업자) 창업진흥원·지자체 등 스타트업 지원 프로그램과 연계하여 보호 교육 확대

○ **(발주담당자)** 시스템 담당자 등이 알아야 할 **PbD 기반** 개발, **처리흐름 분석** 및 영향평가·위험조치, AI·AX 도입시 유의사항* 등 **집중교육**

* 개인정보 생애주기별 고려사항, 비식별화 조치, RBAC 기반 접근권한 최소화 방안 등

□ **(정보주체 생애주기 교육)** **아동·청소년** 및 **디지털 취약계층** 대상으로 개인정보 침해 예방을 위한 **온라인 교육** 및 **찾아가는 교육** 추진

< 대상별 교육 내용(안) >

대 상	교육 내용 예시
아동·청소년	• 앱 권한, 위치정보, 사진·영상 SNS 공유, 계정 보안, 딥페이크·사칭 등 디지털 환경에 맞춘 생활형 교육 • 초·중·고 연계 교육 및 찾아가는 보호 교육 등
청년·성인	• 구직, 금융, 쇼핑, 플랫폼 이용, 생성형 AI 활용 과정에서의 개인정보 자기결정권 행사 방법 안내
고령층·장애인 등 디지털 취약 계층	• 쉬운 언어, 방문형·체험형 교육, 피해예방 중심 콘텐츠 확대

□ **(AI 프라이버시 인식 제고)** AI 서비스 이용과정에서 이용자에게 발생 가능한 주요 프라이버시 이슈 관련 이해를 돕는 정책자료* 마련·배포

* 안전한 AI서비스 이용방법 및 권리 행사 절차 등 실질적인 행동지침 마련·안내

※ AI학습에 이용자 데이터 활용에 대한 동의, 마케팅·정보추천 동의 등 선택시 주의사항 등

※ 사업자 대상 AI 교육과정에 처리 투명성, 신뢰성 확보를 위한 개인정보 보호 필수 반영

2 안심할 수 있는 서비스 환경 조성

□ **(처리방침 개선)** 처리방침의 적정성, 접근성 및 정보주체 권리보장 수준 등을 평가하여 개인정보처리자의 **보호수준 개선 유도**

○ 국민 생활과 밀접하고 **대규모 개인정보·민감정보를 처리**하거나, **신기술 기반 서비스 제공**하는 등 **집중점검이 필요한 분야*** 중심으로 **평가 실시**

* (26년) 공공앱, 대학교, 해외명품브랜드, 채용플랫폼, 만남중개서비스, 프랜차이즈, 팬덤플랫폼 등

- 처리방침 우수사례 **확산, 작성지원 컨설팅** 등을 통해 **자율적 개선 유도**

※ 'AI기반 개인정보 처리방침 통합 지원 플랫폼(가칭)' 구축을 추진하여 일반 개인정보처리자 대상 처리방침 작성 지원, 간이점검 등 지원 추진

○ 아동·청소년, 어르신 등 **정보취약계층**이 쉽게 이해할 수 있도록 **'알기 쉬운 처리방침'을 평가***하여 **처리방침의 투명성·가독성 제고**

* 예: 알기 쉬운 처리방침 보유 여부, 이용자 눈높이에 맞는 처리방침 작성 여부

□ **(신뢰 저해 관행 개선)** 일상 서비스에 대해 과잉수집, 선택권 왜곡, 철회 방해, 불명확 고지 등 **신뢰저해 요소**를 점검하여 **개선 유도**

○ **(민관 협업) CPO 협의회 협업, 분야별 자율개선 활동**과 **연계**하여 프라이버시 보호를 위한 앱·서비스 설정 안내 등 개선

○ **(주제별 사례 전파)** 생활 속 오·남용, 유출사례 및 분야별 개인정보 취급 시 주의사항 등을 주기적으로 안내

□ **(아동·청소년 보호법제 개선)** 권리행사 역량이 취약한 **아동 ·청소년의 특성** 및 **침해 요소**를 고려한 **아동·청소년 보호 법제 개선 추진**

※ **(주요추진내용)** 보호 대상 확대((기존)14세→(개선)19세 미만), 법정대리인 동의 제도 사각지대 해소 및 동의의무 합리화, 디지털 잊힐권리 법제화, 자동화된 결정 제한 등

□ **(신뢰 문화 조성)** 반복되는 유출사고로 누적된 정보주체의 무능감·피로감을 회복하기 위해 '(가칭)**개인정보 신뢰 조성 캠페인**' 추진

○ **(참여형 캠페인) '개인정보 보호 주간'**과 연계하여 국민·기업이 참여하는 범국가적 보호 캠페인 등 자율적 보호문화 확산 도모

* 기념식 개최일이 포함된 9.29.(화)~10.3.(금)까지를 '개인정보 보호주간'으로 운영

※ '개인정보 디톡스' 집중기간 운영, '나만의 개인정보 보안 꿀팁' 숏폼 콘테스트', '정보주체 개인정보 실천 서약' 등 온·오프라인 참여형 개인정보보호 캠페인 진행

○ **(생활속 실천)** 부처·지자체 등과 협업을 통해 생활 속에서 개인정보 보호의 중요성을 인식하고 실천할 수 있는 홍보 활동* 연중 실시

* ATM기기 보호수칙 안내, 지하철·역사 내 홍보, 공문하단 개인정보 보호 슬로건 게시 등

※ 아동·청소년 대상 초·중·고 연계 교육, 노인·장애인 대상 '찾아가는 보호 교육'도 지속 추진

- '개인정보 보호의 날'*(매년 9.30.) 개최를 통해 사회적 **공감대 확산**

* 개인정보보호의 중요성을 알리기 위해 '23년부터 개인정보보호법상 법정기념일로 지정

Ⅴ. 과제별 추진일정

주요 추진과제	추진일정					관련 부처
	’26上	’26下	’27	’28	’29~	
(전략1. 보호체계) 위험 기반(Risk-based) 예방관리체계 구축·운영						
ㅇ 고·중·저 위험군 점검·관리	정기·수시 점검, 합동점검					개인정보위 각 부처
ㅇ 신기술, 사회적 이슈 실태점검	공급망 및 사회적 이슈 점검계획 수립·점검					개인정보위
ㅇ 기초 위험지도 작성	방안 마련		위험지도 구축·확산			개인정보위
ㅇ ISMS-P 인증 실질화	의무화 대상 단계적 확대(’27.7월~)					개인정보위 과기정통부
ㅇ 안전성 확보조치, 영향평가 등 개선	방안 마련		일부 적용(선택)	전면 적용		개인정보위
ㅇ 국외이전 영향평가 도입	도입방안 연구		제도 도입			개인정보위
ㅇ 범부처·민관 협력체계 구축·운영	협의체, 조기경보 연락체계 운영(수시)					개인정보위 과기부,국정원 각 부처
(전략2. 예방투자) 자발적 보안·보호 투자 조기 확대 유도						
ㅇ PbD 원칙, 인증제 도입·확산	보호법 개정안 마련·개정, 인증대상 확대					개인정보위
ㅇ 과징금체계 등 인센티브 재설계	시행령 개정		-			개인정보위
ㅇ CEO 책임경영 및 CPO 독립성 강화	CPO 이사회 의결절차 및 신고의무 도입					개인정보위
ㅇ 개인정보 보호 활동 공개	개인정보 보호활동 공개 방안 마련		운영/확대			개인정보위 과기정통부
ㅇ ‘구독형 컨설팅’ 등 사업자 지원	제도 방안 마련		시범 운영, 제도화 추진			개인정보위
ㅇ 공공부문 역량 확충	필요 예산·인력 기준 산정 관계부처 협의		부처 인력·예산확보 지원			개인정보위 행안부 기획처 재경부
(전략3. 산업기반) 개인정보 보호 산업 기반 활성화						
ㅇ 개인정보보호 강화 기술(PET) R&D	R&D 로드맵 수립		연구개발/실증			개인정보위
ㅇ 공급망 이슈 점검	계획 수립/ 점검, 법적 근거 마련, 가이드 개발					개인정보위
ㅇ 교육프로그램 등 전문인력 양성	석·박사 과정 개설		운영/개선			개인정보위
ㅇ 자격제도 신설	자격 운영방안 마련		자격설계 등 검토	자격 신설		개인정보위
ㅇ 기술분석센터, 디지털포렌식센터 운영	분석센터 구축		분석센터 운영, 기능확대			개인정보위
(전략4. 국민인식) 국민이 체감하는 신뢰 문화 조성						
ㅇ 대상별 교육 확대	대상별 과정 설계		운영/확산			개인정보위
ㅇ 처리방침 개선	평가 실시 및 미흡기업·기관 이행점검					개인정보위
ㅇ 관행 점검·개선 및 사례 전파	다크패턴 점검 주제별 사례 전파					개인정보위
ㅇ 아동·청소년 보호법제 개선	법 개정		법령 개정 후속조치			개인정보위
ㅇ 신뢰문화 조성 캠페인 확산	캠페인 기획	연중 캠페인 실시/개선				개인정보위