개인정보의 안전한 활용과 보호를 위한
인공지능·데이터 사업 개인정보보호 관리체계 개선방안

◈ 본 개선방안을 토대로 각 전담기관은 기관·사업 특성을 반영하여 적용

◈ 사업 전담기관은 사업 수행기관이 개인정보 관련 규정 등을 체계적으로 이행할 수 있도록 적극 뒷받침 필요

□ 배 경

○ **개인정보 활용 인공지능·데이터 사업**이 **증가**하면서, 개인정보보호법 준수 등 **개인정보 보호**에 대한 **사회적 관심 증가**

○ 이에 사업추진 과정에서 **개인정보보호법의 체계적인 준수를 강화**하고 **개인정보 침해 및 유출 가능성**을 사전에 **예방·제거**할 필요

□ 기본 방향

◇ **사업** 全과정에서 **개인정보**의 **안전한 활용과 보호**를 위해 **관리체계 개선**

△ **사업 전담기관의 개인정보보호 관련 지원·점검 확대**

△ **사업 수행기관의 역할과 책임성 강화**

□ 관리체계 개선방안

◇ 전담기관 공동의 **개인정보 활용 과제 자문위원회**' 구성·운영

◇ 과제 기획, 사업공고, 평가·협약, 사업수행, 결과물 활용 등 **사업 全단계별 개인정보의 적법·안전한 처리 적극 뒷받침 및 점검 확대**

1. 전담기관 공동의 '개인정보 활용 과제 자문위원회' 구성·운영

*** '21. 12월 중순 구성 예정**

○ **(구성) 개인정보 전문가**(가명처리, 영향평가 등), **법률 전문가, 관련 전문기관** 등 참여

○ **(운영)** △ **(전담기관 공동)** 매년 사업기획 단계, 중간점검 및 최종점검 등 **정기 개최**, △ **(전담기관별)** 개인정보 이슈 발생 시 **별도로 수시 개최**

○ **(역할) 사업 기획·추진** 시 개인정보 이슈에 대한 **전반적인 사전 검토 및 이슈사항**에 대한 **전문자문** 제공

*** 각 기관별로 세부사업별 상세 자문·점검을 위한 별도의 전문가 풀(Pool) 운영 가능**

2. 사업 全단계별 개인정보의 적법·안전한 처리 적극 뒷받침 및 점검 확대

< 사업단계별 주요내용 >

기획	· **법적 이슈 사전검토**(개인정보 활용 근거, 가명처리 필요 여부, 위탁 처리 필요 여부 등)
공모	· 사업별 특성에 따라 **법적 요건 준수 의무화**(개인정보 동의, 위탁처리 및 고지, 개인정보 영향평가 실시 등) · 개인정보의 적법·안전한 처리를 위한 **각종 가이드라인 및 표준 양식 제공** · 사업 수행기관 담당자의 **사업 착수 전 개인정보교육 이수** 의무화 · **개인정보보호 및 보안 규정 위반 시 제재** 명시
평가·협약	· **개인정보보호법** 및 **실증랩 보안규정 위반 기관**에 대한 **평가시 불이익 강화** · 과제 수행기관이 제출한 **상세 사업계획서 상의 개인정보 이슈 및 조치계획 점검** · 수행기관-전담기관(NIPA, NIA 등) 간의 **역할분담, 책임소재, 손해배상 등 명문화**
수행	· 사업 수행기관 대상 사업 초기·중간 단계에서 **개인정보보호 교육 실시** · (사업 수행기관) **정기적 자체 점검**, (사업 전담기관) **정기적 현장점검 실시**
종료·활용	· 사용된 데이터의 파기, 결과물에 개인정보 포함 여부 점검 등 의무화
실증랩	· 데이터 무단반출 방지 등 **기술적·관리적 대책 마련·시행** * **자동점검 SW 설치**(확장자 변경/압축 금지 등), 반입-반출 시 파일 **변경목록 및 변경내용 제출·확인 등**

❶ 기획단계

◇ 차년도 사업 기획 및 세부 추진계획 수립 단계

○ 각 사업별로 **개인정보를 활용하는 사업인지 여부**, 필요로 하는 **개인정보의 구체적인 내용** 확인

* 개인정보의 세부적인 목록, 개인정보/민감정보/가명정보/익명정보 유형 등

○ **개인정보를 활용하는 사업의 경우**, 개인정보보호법 상 **의무·권고사항 사전점검 및 전문적 자문** 실시

* **(개인정보 주요 점검사항)** 개인정보 수집·활용·제공 등에 대한 법적 근거, 목적 외 사용 금지 위반 여부, 위탁처리 또는 제3자 제공 여부, 개인정보 영향평가 대상 여부, 가명처리 필요 여부, 결과물 지식재산권 등

* **(윤리적 이슈)** 개인정보 처리와 관련된 윤리적 이슈가 발생하는지 점검(사회적 편향/차별, 사생활 침해/차별 등)

* **(참고자료) 인공지능 개인정보보호 자율점검표**(개인정보위, '21.5), 생체정보 보호 가이드라인(개인정보위, '21.9), 가명정보 처리 가이드라인('21.10) 등

→ 필요시 법률자문, 개인정보위 유권해석 의뢰, KISA 문의 등 실시

❷ 사업공모 단계

◇ 해당 사업을 수행할 기관·기업 등을 공모하는 단계

○ **공모안내서**에 **사업별 특성을 고려**하여 **법적 요건 준수 의무화 반영**

- **'❶ 기획단계'에서 확인된 사항** 중 의무사항·권고사항을 구분

* **자유공모 과제의 경우**, 사업 제안기관이 제안 내용이 개인정보보호법 등 관련 법률 및 규정 상 문제가 없음을 확인하는 내용의 법률 검토결과(자체검토 포함)를 사업 제안서에 필수적으로 제시 (개인정보 수집·활용·제공 근거, 가명처리 여부, 위탁처리 여부, 영향평가 대상 여부 등)

* 특히, 아래사항 의무화 필요

- 위탁처리 시 위탁협약 체결 즉시, 위탁처리 사실 고지 의무화
- 개인정보 영향평가 대상인 경우, 사업 착수와 동시에 개인정보 영향평가 공모 의무화
- 가명처리가 필요한 경우, '가명정보 처리 가이드라인' 준수 의무화

- 활용되는 **개인정보의 구체적인 내용 및 관련 규정의 이행·점검·조치 방안** 등을 과제 제안서에 필수적으로 포함

○ **공모 안내서**에 사업 수행기관의 **개인정보보호법 위반, 실증랩(안심존) 보안규정 위반 시, 제재처분**을 구체적으로 명시

* 사업별 특성을 반영하되, 고의 및 중대한 위반 사항 등의 경우는 **사업협약 해지 및 사업비 환수 등 엄격한 제재** 필요

* 특히, **실증랩 외부로의 데이터 무단반출**의 경우, 확인 즉시 사업협약 해지 및 사업비 환수 조치

○ **평가 기준** 관련, 사업 제안기관·기업의 과거 개인정보보호법 위반, 실증랩(안심존) 보안규정 **위반이력 제출 의무화** 및 **평가시 불이익 반영**

* 사업별 특성을 반영하되, 고의 및 중대한 위반 사항 등의 경우는 **사업 참여에 실질적인 불이익**이 발생하도록 평가기준 설정(감점 등) → **전담기관 사업관리 지침에 근거 규정을 마련**하고, 개인정보 활용 개별 사업 별로 탄력적으로 적용

< 개인정보 보호 위반 기업에 대한 사업참여 평가 방안(안) >

· **(사업)** '22년 개인정보 활용 사업(전담기관별)

· **(적용기준)** 공고일 기준 **2년 이내***에 개인정보 보호 위반으로 전담기관으로부터 **중대한 제재처분**(협약해약, 사업비 환수 등)을 **받은 기업**

· **(불이익 수준)** 타사업 형평성을 고려하여 **전담기관 자체적으로 감점 기준 설정****

* (국가연구개발혁신법 시행령 제12조) 보안사항 등 위반기관 2년 이내 불이익

** (기금사업 협약체결 및 사업비 관리 등에 관한 지침) 전담기관은 평가기준(우대·감점 등) 수립 가능

○ 사업 수행기관(주관, 참여기관 포함)의 담당자들의 **사업 착수 전 개인정보보호 교육 이수 의무화**

○ 사업 수행기관이 개인정보 관련 규정 등을 **체계적으로 준수**할 수 있도록 **기본 가이드라인, 표준 양식 등을 제공**하여 **적극 뒷받침**

* 기본 가이드라인 및 표준 양식은 개인정보위 등에서 기 발행한 자료를 토대로 인공지능·데이터 **사업별 특성을 고려하여 구체화·수정하여 활용**

○ 가명정보로부터 특정 개인정보가 식별될 경우 이에 대한 관리적·기술적 조치사항 및 프로세스를 마련하고 가명정보 처리·제공·활용 관련 계약, 실증랩 운영규정 등에 명시적으로 반영 안내

< 개인정보보호 관련 기본 가이드라인 및 표준양식(붙임 참조) >

o 인공지능 개인정보보호 자율점검표(개인정보위, '21.5.), 공공기관용 개인정보 보호 법령해석 실무교재를 중심으로 개별 사업에 필요한 각종 가이드라인* 제공(개인정보위, '21.11.)

* 생체정보 보호 가이드라인(개인정보위, '21.9), 가명정보 처리 가이드라인(개인정보위, '21.10), 개인정보 처리방침 작성 가이드라인(개인정보위, '20.12), 개인정보 수집최소화 가이드라인(개인정보위, '20.12, 개인정보 수집제공 동의서 작성 가이드라인 포함), 영상정보처리기기 설치운영 가이드라인(개인정보위, '21.4), 개인정보 영향평가 수행 안내서(개인정보위, '20.12), 개인정보처리 위수탁 안내서(개인정보위, '20.12), 개인정보암호화 조치 안내서(개인정보위, '20.12), 개인정보 유출 대응 매뉴얼(개인정보위, '20,12), 개인정보 침해요인 평가 지침(개인정보위, '21.12) 등

❸ 사업 수행기관 평가 및 협약 단계

◇ 사업 수행기관을 평가 및 협약하는 단계

○ 과거 개인정보보호법 위반, 실증랩(안심존) 보안규정 위반 기관·기업 등은 **평가 시 불이익 처리**

○ 사업 수행기관이 제출한 **사업수행 계획서**(제안서)에 포함된 **개인정보 관련 규정 이행·점검·조치방안 검토 → 미흡한 사항 보완 요청**

○ 개인정보보호법상 개인정보처리자인 **사업 수행기관**(부처, 지자체, 공공기관, 기업 등)과 **사업 전담기관**(NIPA, NIA 등) 간의 **개인정보 보호법상 역할분담, 책임소재, 손해배상 등 명시**

< (예시) 인공지능 학습용 데이터 사업 점검 사항 >

o 인공지능 학습 등에 개인정보가 포함된 데이터를 사용하는지 여부
  * 개인정보(가명정보·생체정보 등), 초상권 등 포함 및 침해 여부 점검

o 개인정보 영향평가 대상 여부, 기 수행 혹은 수행 예정 여부, 수행 계획이 일정상 무리가 없는지 등

o 학습데이터 등의 획득(촬영승인 여부, 관련 법률 위반 여부 등), 활용이 적법한 절차(비식별화(가명, 익명화 등))에 따라 진행되는지를 확인
  - 가명정보를 처리하는 경우 허용된 목적•기준 준수 여부 체크

o 수집목적 내 개인정보 이용(개인정보위탁), 제3자 제공, 목적외 제공인 경우 별도 근거가 있는지 등 개인정보 활용에 대한 근거 확인
  * 개인정보 위탁의 경우 관리사항 문서화, 수탁자 교육 및 관리감독, 위탁사항 공지 등을 수행하는지 확인

o 개인정보처리방침의 투명한 공개, 이용자의 권리 행사요구에 대한 절차 마련 및 이행, 개인정보 유출시 정보주체 통지, 관계기관 신고, 피해구제 절차 등이 마련되어 있는지 검토

o 기타 법률검토, 개인정보보호위원회 의견조회 필요 여부 등을 검토

❹ 사업 수행 단계(종료 단계 포함)

◇ △ **사업 수행기관**은 정기적으로 **자체 점검** 후 **전담기관에 결과 보고,**
△ 사업 **전담기관**(NIPA 등)은 **정기적으로 현장점검** 실시

○ **(교육) 사업 착수 시**(Kick-off), 사업 수행기관 대상 **개인정보보호 및 보안관리 관련 교육** 실시

* 전담기관(NIPA 등)의 사업 관리 담당직원 대상으로도 개인정보보호 교육 이수 의무화(법정 의무교육)

○ **(점검) 사업 제안서 상의 개인정보 관련 내용** 및 **'인공지능 개인정보보호 자율점검표(개인정보위, '21.5)'**를 중심으로 점검

- **사업 중간·최종 점검 시 개인정보보호 전문가**를 통해 점검

* 법무법인·개인정보영향평가 전문기관 등을 선정·계약하여 개별 사업별 점검 업무 수행

- **필요시** 전담기관 주도로 **개인정보 전문가**(비식별, 영향평가 등), **법률 전문가** 등이 참여하는 **'점검단'을 구성**하여 **점검 실시**

< 데이터를 개방하는 사업의 경우 추가 절차 >

○ 데이터를 개방하는 사업의 경우 개방전 개인정보(전화번호, 주민번호 등) 포함 위험이 큰 데이터를 선정하여 전수 조사 실시

* 상담, 고객 정보가 포함된 각종 대화 데이터, 차량 이미지 및 영상, 사람이 많이 촬영된 CCTV 영상 데이터 등

- 데이터를 구축한 **사업수행기관을 통해 데이터 전수 검수 및 개인정보 비식별 조치 실시(1차)**
- 수행기관이 누락한 개인정보가 존재할 수 있으므로, 사업 전담기관(NIA 등) **자체 검사** 및 **전문기업**을 통해 **개인정보 재검증 및 조치(2차)**
- 솔루션을 통한 검증 과정에서 **식별되지 않은 개인정보***는 **육안검사**를 통해 식별하여 **비식별 또는 삭제 조치(3차)**

* 예시) 공일공 XXX X XXXX(X: 숫자 발음 전사)와 같은 불규칙 패턴을 가진 데이터

- 개인정보 비식별화 조치가 완료된 데이터는 사업 전담기관(NIA 등) **및 전문기업이 개인정보 비식별화 누락 여부를 최종 확인**한 다음 **개방**

❺ 결과물 활용 단계

◇ 사업 종료 이후 인공지능 제품·서비스를 활용하는 단계

○ 사업 종료 후 인공지능 **사업 결과물(알고리즘 등)에 개인정보가 포함되어 있는지 등을 확인**

- 사업 종료 이후 개인정보가 포함된 **학습데이터의 파기를 확인**하고 이를 **보관할 경우 이에 대한 법적 근거가 있는지** 등 확인
- 사업 종료 이후 인공지능 사업 결과물이 **윤리적 이슈를 유발하는지 등을 지속 점검**

< 데이터를 개방하는 사업의 경우 추가 절차 >

○ 개방 후 **개인정보 탐지 소프트웨어(2종 이상)*** 등을 활용하여 **주기적**으로 개인정보 포함 여부 **재검증 정기 실시**

* 개인정보(이름, 성별, 주민등록번호, 전화번호, 주소 등) 패턴 식별 및 탐지 기능

- **분기별/반기별 데이터 정기검증**을 수행하고 개인정보 등의 탐지 결과에 대해 데이터 구축 **수행기관에 즉각 보완조치 요청**

❻ (기타) 실증랩(안심존) 보안관리 강화

◇ 데이터의 안전한 활용·보호를 위한 강화 대책 적용

○ 데이터 무단반출 방지 등 **기술적·관리적 대책** 강화·시행

* '개인정보의 기술적·관리적 보호조치 기준 해설서(개인정보위, '20.12월)'를 토대로 개별 사업 별 실증랩, 안심존의 특성을 반영하여 구체화하여 시행

< 실증랩 보안관리 강화방안(안) >

◈ **개인정보 데이터 반출**은 금지하고, 인공지능 모델·알고리즘 등은 **보안 전문가**가 **점검** 후 제한적으로 반출 허용

* 개인정보 데이터 반출입 및 관리·활용에 관한 책임·의무 등 세부사항은 제공기관과 활용기관 간 협약을 통해 책임 및 의무사항 규정

** 개인정보보호 자체 교육 실시, 개인정보보호·보안 전문가를 통한 자체 점검 등

○ **(접근통제)** 입·출입자 통제 및 기록, 업무·작업 승인 및 기록, 사용자 ID 관리, 시스템에 대한 사용 권한 체계 마련, 서버접근용·개발용 PC(USB 봉인) 분리

○ **(반출관리)** 관리서버를 통한 파일 반출 관리 및 보안 USB 사용 권장 등

* AI 알고리즘 반입-반출 시 파일 변경목록 및 변경내용 제출·확인절차 의무화 등

○ **(네트워크)** 이중화(인터넷망, 패쇄망), 데이터 서버에 대한 접속 물리적 차단

○ **(SW)** 화면 캡쳐·저장 방지 프로그램, 자동점검 SW 설치(확장자 변경/압축 금지 등)

* 필요시 개인정보 및 주요 보안 데이터 암호화