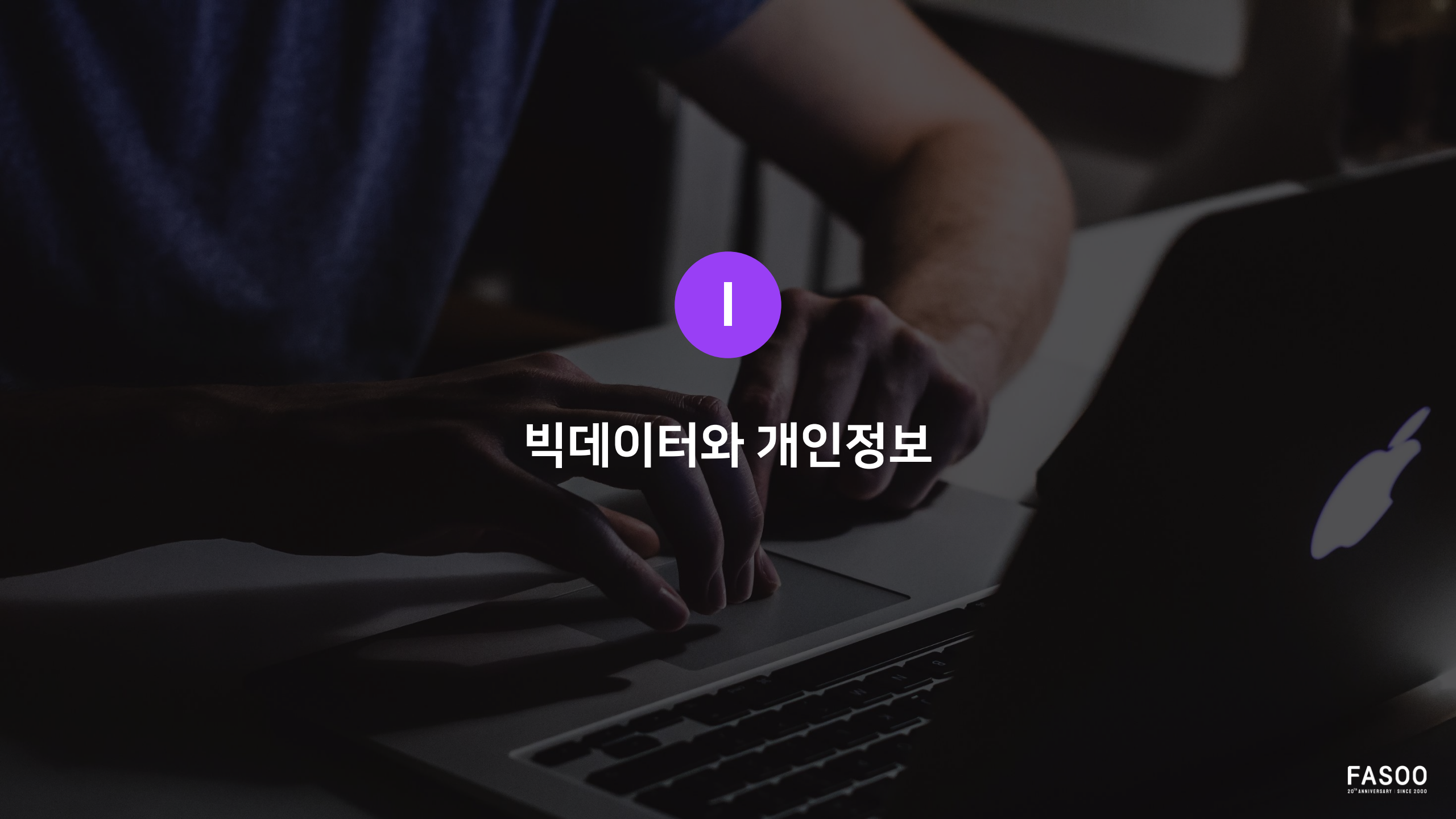
빅데이터 비즈니스의 핵심

개인정보 안전한 활용 지원 비식별 솔루션

윤덕상 전무

FASOO
20TH ANNIVERSARY SINCE 2000



I

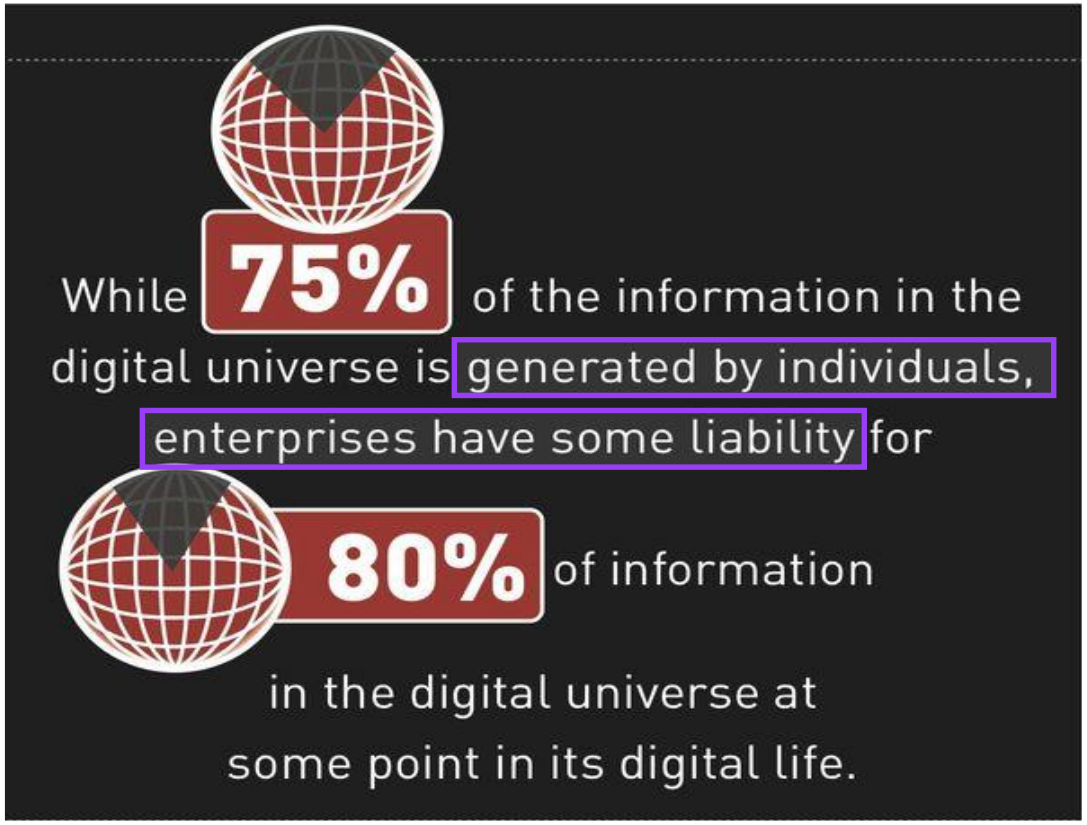
빅데이터와 개인정보

4차 산업혁명의 에너지원은 데이터

이코노미스트

"세상에서 가장 가치있는 자원은
더 이상 기름이 아니라 데이터이다!"

디지털 정보의 75%는 개인에 의해 생성된 정보



Source: IDC Digital Universe Study

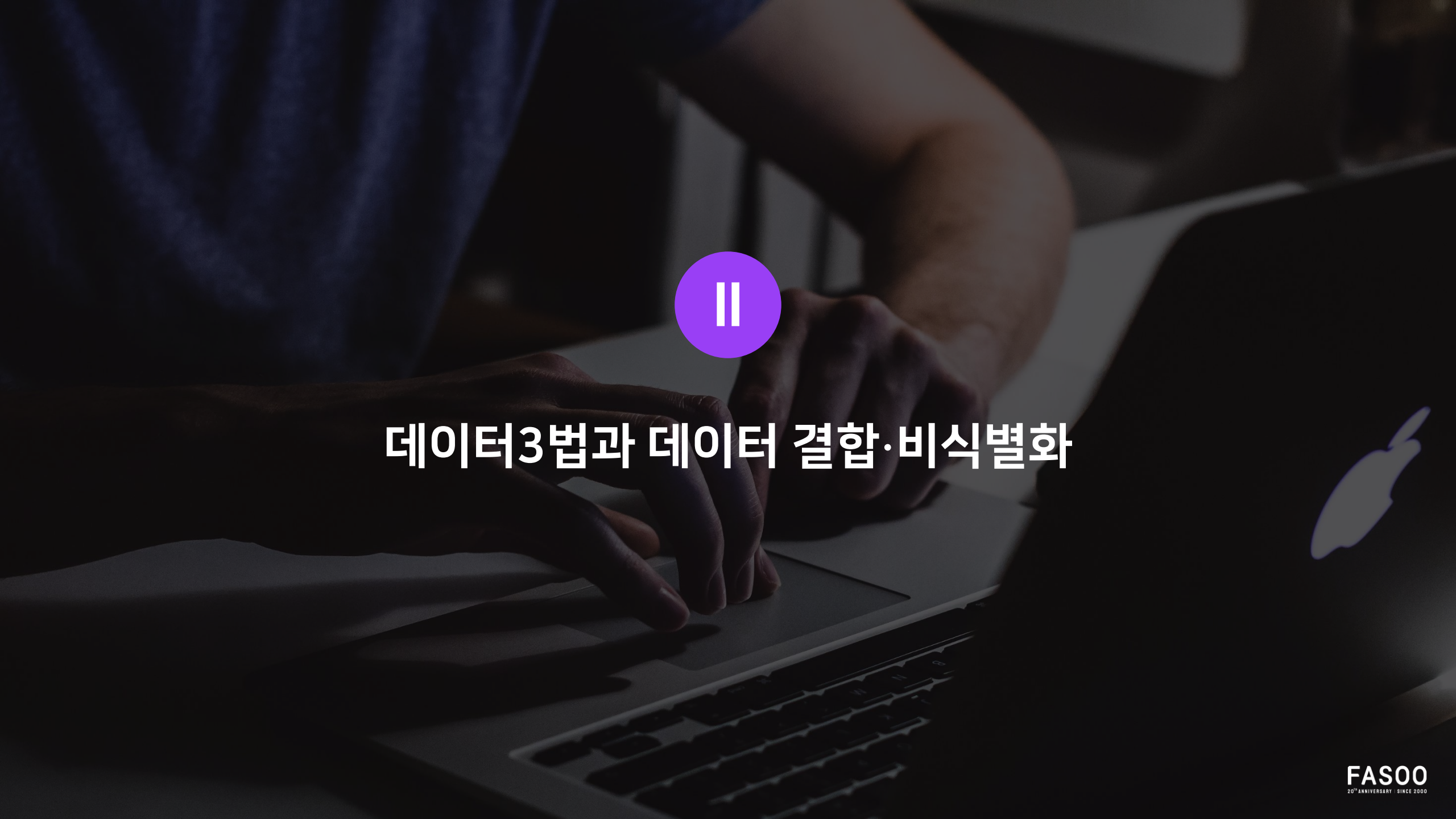
개인정보 데이터의 양면성

안전하게 잘 사용하면

- 데이터 기반 신 사업 창출
- 4산업혁명의 획기적 발전
- 각종 연구 기술 발전 기여
  - 질병, 보건, 의료, 유전자 분야
  - 인공지능, 딥러닝 분야
  - 제조설비 자동화
- 유통, 서비스 산업의 활성화
- 개인 맞춤형 정보 서비스 발전

잘못 사용하면

- 개인정보 유출
- 사생활(Privacy) 및 인권침해
- 개인정보의 불법적 활용
- 불법적 마케팅, 통계 활용
- 금전적, 재산상 피해
- 종교적, 정치적, 사상적 차별
- 개인 평판, 신용 추락



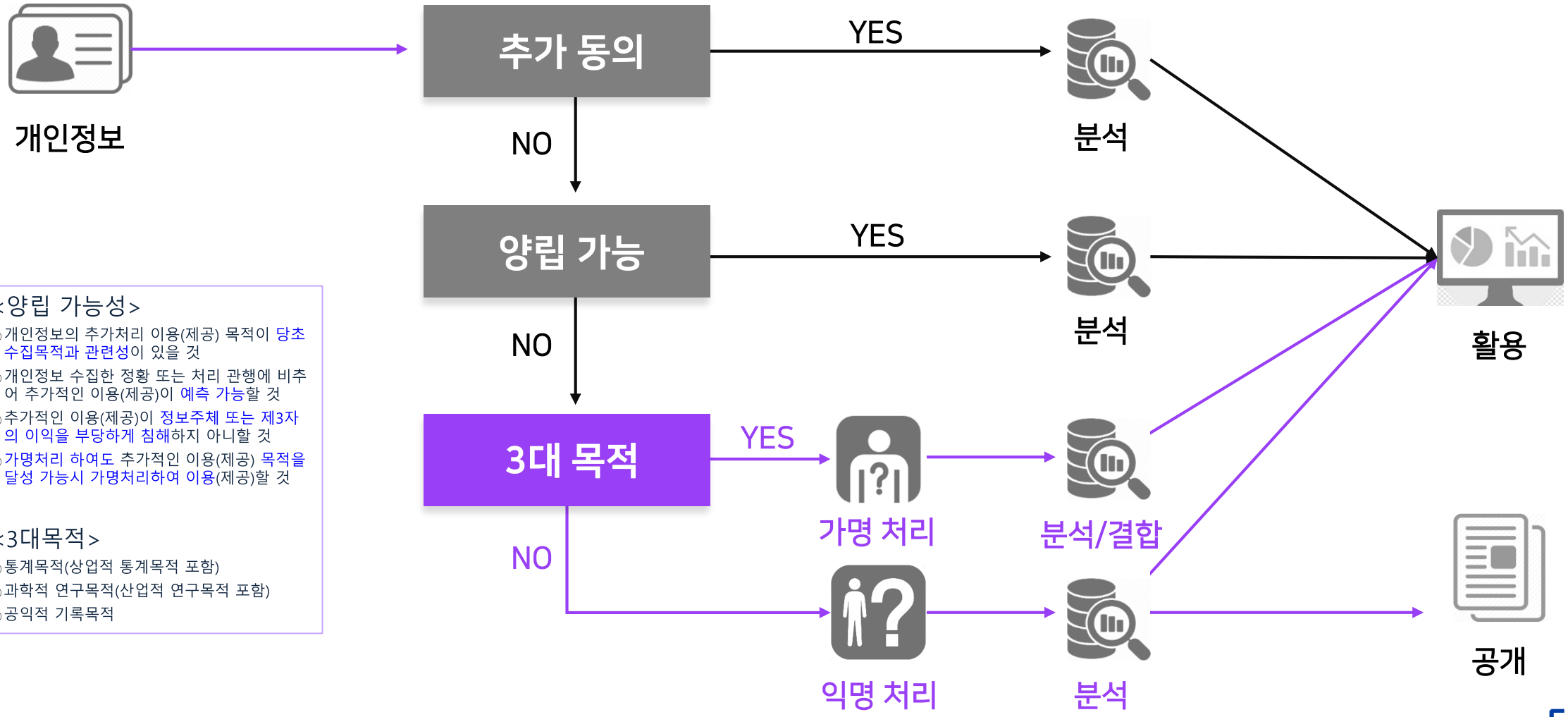
II

데이터3법과 데이터 결합·비식별화

데이터 3법 개정안 핵심사항 (1/2)

기존	**당초 수집 목적 외 개인정보 활용 불가** (필요시 추가 동의 후, 이용가능)
개정	**당초 수집 목적 외 개인정보 활용 가능** (추가 동의 없이 이용 가능)

데이터 3법 개정안 핵심사항 (2/2)



<양립 가능성>

① 개인정보의 추가처리 이용(제공) 목적이 당초 수집목적과 관련성이 있을 것

② 개인정보 수집한 정황 또는 처리 관행에 비추어 추가적인 이용(제공)이 예측 가능할 것

③ 추가적인 이용(제공)이 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니할 것

④ 가명처리 하여도 추가적인 이용(제공) 목적을 달성 가능시 가명처리하여 이용(제공)할 것

<3대목적>

① 통계목적(상업적 통계목적 포함)

② 과학적 연구목적(산업적 연구목적 포함)

③ 공익적 기록목적

개정 개인정보보호법 및 시행령

가명화, 익명화 개념 도입

(법 제2조 제1호, 제58조의 2)

- 가명 정보 : 개인을 알아볼 수 있는 정보 또는 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보를 가명 처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용 결합 없이는 특정 개인을 알아 볼 수 없는 정보
- 가명 처리 : 개인정보의 일부를 삭제 하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것
- 익명 정보(제58조의2) : 시간·비용·기술 등을 합리적으로 고려 할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보 (개인정보보호법 적용대상이 아님)

구분	개념	활용 가능 범위
가명 정보	추가 정보의 사용없이 특정 개인을 알아볼 수 없게 조치한 정보	① 통계 목적(상업적 목적 포함) ② 과학적 연구 목적(산업적 연구 포함) ③ 공익적 기록 목적 등
익명 정보 **(제58조의 2)**	더 이상 개인을 알아 볼 수 없게 (복원 불가능한 정도로) 조치한 정보	개인정보가 아니기 때문에 제한없이 자유롭게 활용 가능

- **가명처리시 하기 규정에서 제외**

수집출처고지, 개인정보파기, 양도에 따른 개인정보 이전 제한, 유출통지, 열람·정정·삭제 요구,
(망법)유출통지, 파기, 이용자 권리, 개인정보 이용내역 통지 등

가명 정보의 안전조치 의무

(법제 28조의 4, 시행령 안 제 29조의 5)

개인정보보호법	시행령	파기 의무 (시행령)
• 원래의 상태로 복원하기 위한 추가정보를 별도로 분리하여 보관·관리 • 해당정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치 • 가명정보의 처리 목적, 제3자 제공시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 함	• 내부관리계획 수립, 추가정보 별도 분리보관, 추가정보 접근 권한 분리, 가명정보/추가정보 접근 기록 관리, 물리적·기술적 안전조치 실시 • (내부관리계획) 개인정보 보호책임자 지정, 취급자에 대한 교육, 접근 권한 관리 및 접근 통제, 접속기록 보관 및 점검에 관한 사항 등 포함(안전성 확보조치 기준 제4조) • 가명정보 처리 목적, 보유기간, 이용 및 파기 등 내용의 작성 및 보관(보호위가 정하여 고시하는 사항)	• 가명 정보의 처리 목적이 달성되거나 보유 기간이 경과하면 지체없이 파기하도록 하

가명 처리 가이드라인 작성 계획

(2020년 6월 11일 발표, 가이드라인 최종안은 보호 위 출범 후 공개 예정)

구성 및 작성 체계

- (구성) 가명 처리 가이드라인, 가명 정보 결합 및 반출 가이드라인 각 1종
- (작성 체계) 보호위원회 집필(KISA 지원), 자문위원회* 구성 · 운영 (학계 · 법률 · 기술전문가 등 외부전문가로 구성)

작성 원칙

- 가명 처리 수준은 처리 환경에 따른 재 식별 가능성 등을 고려하여 스스로 판단하도록 함
- 개정 법률에 따른 규정을 구체적으로 설명하고, 가명·익명 처리 기술에 대해 기술 중립성에 입각하여 작성 (가명 처리 방법 등 예시는 Negative방식으로 작성)
- 보호위원회 작성 가이드라인에는 일반적인 사항 및 절차를 수록하고,
- 필요시 보호위원회와 소관부처가 협의하여 분야별 특수성을 반영한 가명처리 예시 등을 수록한 분야별 가이드라인 별도 발간

가명 처리 가이드라인

- 가명 처리 절차
  - 사전준비 : 가명 처리 목적 명확화 및 대상(최소 처리 원칙 준수) 선정
  - 가명 처리 : 처리 환경(내부 사용, 제3자 제공 등)을 고려한 가명 처리
  - 수준 설계, 가명 처리 실시
  - 가명 정보 적정성 검토 : 설계에 따른 가명 처리 결과의 적정성 판단
  - 추가 처리 : 미흡한 사항에 대한 추가 가명 처리(2,3단계 반복 수행)
- 가명 정보의 안전한 관리 : 법령상 안전조치 의무에 대한 안내
- 참고자료
  - 가명 · 익명 처리 기술 : 주요 가명 · 익명 처리 기술 안내 및 적용 예시
  - 가명 정보 처리 환경에 따른 유의사항 및 예시 : 처리 환경에 따른 가명 처리 방법 및 예시

가명 정보 결합 및 반출 가이드라인

- 사용자 편
  - 결합 신청 : 결합 신청 방법, 전문기관과 사전협의 방법 및 내용, 사전 결합률 확인요청 서비스 이용 안내
  - 가명 정보 제출 : 결합 전 가명 처리 및 결합키 생성 지원에 관한 사항, 결합키 및 가명 정보 전송 방법
  - 가명 · 익명 처리 및 분석, 반출 : 분석 공간 이용 절차, 반출 절차 및 승인 심사에 필요한 사항
- 전문기관 편
  - 결합 신청 : 결합 신청 접수 시 업무절차 및 확인 사항
  - 결합 : 결합 신청서 확인 사항, 결합키관리기관과의 업무처리 절차
  - 분석 공간 제공 및 반출 : 분석 공간 제공에 관한 사항, 반출 심사 위원회 구성 및 반출 절차 등
  - 전문기관 관리 · 감독 : 전문기관 관리 · 감독 관련 규정, 주기적 보고사항 안내, 결합 및 반출 관련 기록 보관 의무

신용정보보호법, 시행령, 고시

가명 정보의 개념 및 행위규칙

(법 제2조 제15호~17호, 제26조의4, 제40조의 2, 영 제34조의5)

가명 정보, 익명 정보 개념

- 가명 정보 : 추가정보를 사용하지 아니하고는 특정 개인을 알아볼 수 없도록 처리(가명 처리)한 개인신용정보로서 가명 정보의 개념을 도입 (제2조제15호, 제16호 신설)

  다음의 경우도 특정 개인인 신용정보주체를 알아볼 수 없도록 처리한 경우에는 가명정보에 포함
  가. 어떤 신용정보주체와 다른 신용정보주체가 구별되는 경우
  나. 하나의 정보집합물에서나 서로 다른 둘 이상의 정보집합물 간에서 어떤 신용정보주체에 관한 둘 이상의 정보가 연계되거나 연동되는 경우

- 통계작성(시장조사 등 상업적 목적의 통계 작성을 포함(개보 법에는 없는 내용)), 연구(산업적 연구를 포함), 공익적 기록 보존을 위해서는 가명 정보를 신용정보주체의 동의 없이도 이용하거나 제공할 수 있도록 규정 (제32조제6항 제9의2, 제9의4)

- 익명 정보 : 금융위원회에서 지정한 데이터 전문기관의 적정성 평가를 거친 경우(개보 법에 없는 내용)에는 더 이상 특정 개인을 알아볼 수 없도록 처리한 정보로 추정하여 금융회사 등의 빅데이터 활용에 따른 법적 불확실성을 어느 정도 해소 (제2조제17호, 제26조의4, 제40조의2 제3항부터 제5항까지)

가명 처리 행위 규칙

- 가명 처리한 개인신용정보에 제3자가 불법적으로 접근하는 것을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치· 운영에 관한 사항
- 가명 처리한 개인신용정보의 변경·훼손 및 파괴를 방지하기 위한 사항
- 가명 처리한 개인신용정보 취급·조회 권한을 직급별·업무별로 차등 부여하는 데에 관한 사항 및 가명 처리한 개인신용정보 접근 기록의 주기적인 점검에 관한 사항
- 가명 처리 전 개인신용정보와 가명 처리한 개인신용정보의 분리에 관한 사항
- 통계작성, 연구, 공익적 기록보존 등을 위하여 가명 정보를 제공하는 경우 해당 목적 외 활용 방지에 관한 사항

- **가명처리시 하기 규정에서 제외**

  개인신용정보 누설통지, 제3자제공 사실고지, 전송요구권, 이동/제공사실조회, 신용정보 제공/이용 통지 등

가명 정보에 관한 보호조치 기준 (1/2)

(고시 제 43조의 7)

가명 정보에 대한 기술적 · 물리적 보호조치

① 가명처리전정보와 가명처리한정보를 분리 저장

② 가명 정보 취급 담당자 별도로 지정 · 관리하고 개인신용정보 취급 담당자와 접근권한 구분 운영

③ 가명 정보 취급 직원은 원본 정보에 접근 불가하며, 불가피한 경우 관리책임자의 사전 승인 후 일시적 접근 및 관련 기록 보관 등 적절한 통제시스템 구축

④ 기록 보관시 접근자의 신원, 관리책임자의 신원, 접근일시, 대상정보 접근이 불가피한 사유, 용도 등의 기록을 3년 이상 보관

⑤ 가명 처리 시 구체적인 처리 목적, 처리 방법, 처리 일시를 기록하여 가명 정보가 파기된 이후 3년 이상 보관하고, 처리 기록에 대해 월 1회 이상 주기적으로 확인 · 감독

⑥ 가명 정보 오·남용에 대한 자체 제재기준을 마련

추가 정보에 대한 기술적 · 물리적 보호조치

① 추가정보를 삭제하지 아니하고 보존하여야 하는 경우 가명 정보와 분리된 저장소에 암호화하여 저장

② 가명 정보를 취급하는 직원은 추가 정보에 접근금지, 불가피한 경우 관리책임자의 사전 승인 후 일시적 접근, 관련 기록 보관 등 적절한 통제 시스템 구축

③ 기록 보관시 접근자의 신원, 관리책임자의 신원,접근일시, 대상정보, 조회가 불가피한 사유, 용도 등의 기록을 3년간 보관

④ 추가 정보가 가명 정보를 재 식별하는 데 사용되는 등 부정한 목적으로 사용되지 않도록 월 1회 이상 주기적으로 점검

가명 정보에 관한 보호조치 기준 (2/2)

(고시 제 43조의 7)

가명 정보에 대한 관리적 보호조치

① 가명 처리한 개인신용정보에 대하여 가명 정보를 보호하기 위해 별도 내부관리계획을 수립 · 시행

1) 가명 정보 및 추가 정보에 대한 접근 권한 부여 · 변경 · 말소에 관한 사항
2) 가명 정보 및 추가 정보가 저장 또는 처리되는 시스템 · 단말의 보호조치에 관한 사항
3) 가명 정보 및 추가 정보에 대한 접근 기록 보관 및 점검에 관한 사항
4) 가명 정보 및 추가 정보의 보유 기간 및 파기 기준 · 방법에 관한 사항
5) 가명 정보의 목적 외 활용 방지 및 재 식별 방지 대책에 관한 사항
6) 가명 정보 제3자 제공 시 사후관리에 관한 사항

① 가명 정보 및 추가 정보에 접근하는 취급자들에 대해 가명정보보호 교육을 연 1회 이상 수행

1) 가명 정보의 목적 외 활용 금지에 관한 사항
2) 가명 정보의 재 식별 금지에 관한 사항
3) 가명 정보 재 식별 시 즉시 회수 및 삭제에 관한 사항

③ 가명 정보의 보존 기간을 주기적으로 검토하고, 그 적정성 여부를 판단하여 필요시 조정

④ 가명 정보를 제3자에게 제공하는 경우 다음 각 호의 사항을 준수

1) 가명 정보를 불특정 다수에게 공개하지 아니할 것
2) 가명 정보 제공 시 가명 정보를 제공 받는 자, 가명 정보 활용 목적, 가명 정보 이용·보존기간 등을 구체적으로 명시하여 제공할 것
3) 가명 정보의 재 식별 금지, 가명 정보의 목적 외 사용 금지 등 관련 법령 준수에 관한 사항을 주지시킬 것
4) 추가정보를 제공하거나 공개하지 않을 것
5) 가명 정보의 재 식별 가능성을 발견한 경우에는 즉시 그 정보를 처리하고 있는 자에게 통지하고 처리 중단 요구 및 해당정보를 회수 · 파기하는 조치를 취할 것

결합 전문기관(개보법 기준)

결합 전문기관 법적 근거

(법 제 28조의 3, 영 제 29조의 2)

법 제28조의3(가명 정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명 정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명 정보 또는 제58조의 2(익명 정보)에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.

가명 정보 결합
(시행령 제29조의2의 제2항)

② 결합전문기관은 특정 개인을 알아볼 수 없도록 보호위원회가 정하여 고시하는 절차와 방법에 따라 가명 정보를 결합하여야 한다. 이 경우 보호위원회는 결합전문기관이 특정 개인을 알아볼 수 없도록 하는데 필요한 지원업무를 한국인터넷진흥원이 수행하도록 할 수 있다.

결합 정보의 분석
(시행령 제29조의2의 제3항)

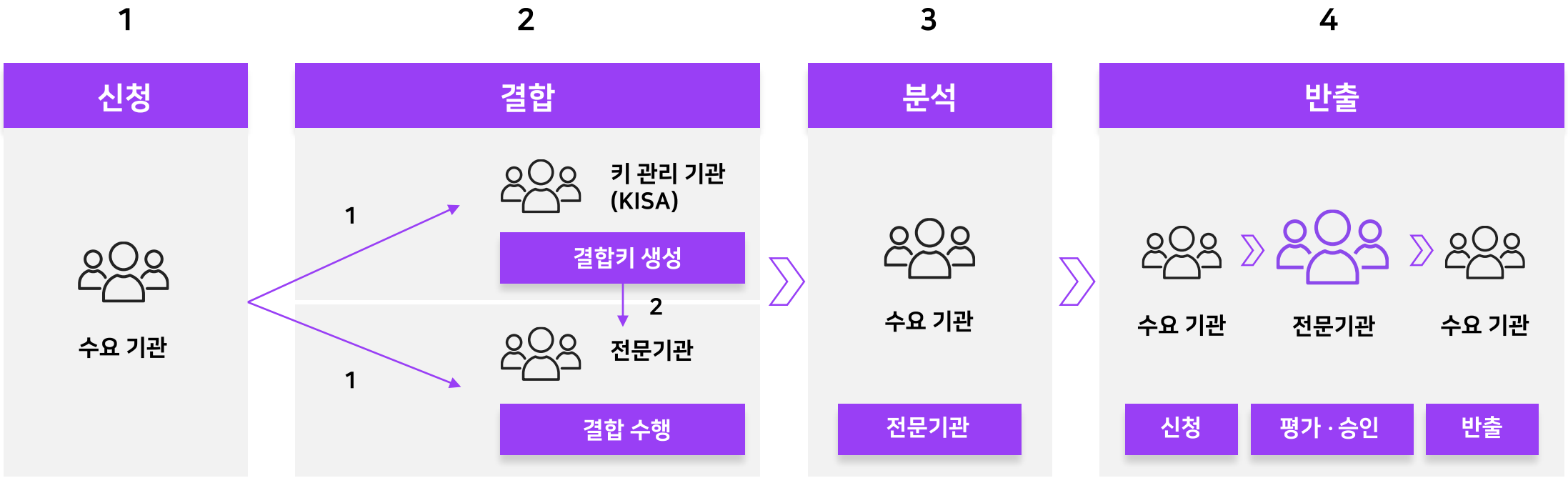
③ 결합신청자는 보호위원회가 정하여 고시하는 바에 따라 결합전문기관에 설치된 안전성 확보에 필요한 기술적·관리적·물리적 조치가 된 공간(이하 "분석 공간" 이라 한다)에서 제2항에 따라 결합된 정보를 분석할 수 있다.

결합 정보의 반출
(시행령 제29조의2의 제4항)

④ 제3항에도 불구하고 분석공간에서는 결합 목적을 달성하기 어렵거나 분석 공간의 이용이 어려운 경우로서 결합신청자가 제2항에 따라 결합된 정보의 반출을 신청하는 경우, 결합전문기관은 개인을 다시 알아볼 가능성 등을 고려하여 보호위원회가 정하여 고시하는 바에 따라 평가한 후 반출을 승인할 수 있다.

가명 정보 결합 및 반출

(법 제 28조의 3, 시행령 제 29조의 2, 제 29조의 3, 제 29조의 4)



결합전문기관 안정성 확보 조치

(고시 제13조)

파기 및 기록보관

① (결합전문기관) 안전한 가명 정보의 처리를 위하여 다음 각 호의 사항을 이행

1. [별표1]에 따른 결합전문기관 지정 기준 준수
2. 법 제29조 및 영 제30조제1항·제2항에 따른 안전조치
3. 비인가 인력·장치·정보의 접근을 제한하기 위한 안전조치
4. 결합된 정보의 유출을 방지하기 위한 안전조치

② (결합전문기관) 가명 정보의 분석 또는 반출 이후에는 가명 정보의 결합·반출과정에서 제공받거나 생성한 정보를 지체없이 파기하여야 함. 단, 다음 각 호의 사항은 보관

1. 결합·반출 신청서 및 첨부 서류
2. 반출 심사에 대한 결과 및 심사위원 명단
3. 분석 공간 이용 관련 결합신청자의 보안 서약서
4. 결합 정보 및 심사 대상 정보에 대한 파기 대장

③ (결합전문기관) 보호위원회가 요청할 경우 제2항 각 호의 기록을 제출 하여야 함

④ (결합키관리기관) 결합키생성정보와 결합 키가 불필요하게 된 때에는 지체없이 파기

공간 및 시설 장비구축

- 안전한 결합대상정보의 수신 및 반출 정보의 송신 시스템 (네트워크, 데이터)
- 가명 정보 결합 시스템
- 분석 및 반출 심사를 위한 독립 공간 및 물리적 안전 시설·장비
- 가명·익명 처리 및 통계처리 등을 위한 HW·SW
- 반출 심사를 위한 HW·SW
- 관련 정보의 완전한 파기를 위한 SW
- 결합 및 반출 관련 기록·보관 시스템
- 네트워크, 시스템 및 정보의 보호를 위한 시설·장비
- 클라우드 활용 시 클라우드 보안 인증을 받은 서비스 이용

정책 및 절차 마련

- 결합, 분석, 반출 심사(심사위원 구성 포함) 등 업무수행 정책 및 절차
- 개인정보의 안전성 확보 조치 기준 제4조제1항 제4호부터 제9호까지 대한 내부관리계획
  (4. 접근 권한의 관리에 관한 사항, 5. 접근 통제에 관한 사항, 6. 개인정보의 암호화 조치에 관한 사항, 7. 접속기록 보관 및 점검에 관한 사항, 8. 악성프로그램 등 방지에 관한 사항, 9. 물리적 안전조치에 관한 사항)
- 가명 정보 유출사고 대응 계획
- 결합·반출 관련 정보의 파기 및 기록·보관에 대한 정책 및 절차
- 분석 및 반출 심사 공간에 대한 반출 입 정책·절차
- 운영 인력에 대한 교육계획

전담 조직의 구성·운영 및 자격조건

- 3명 이상이 상시 고용되어 있는 전담 조직의 구성·운영(분야별 고루 포함되도록)
- 기술자, CISA, CISSP, ISMS-P심사원, 박사학위, 변호사 자격 취득한 후 3년 이상
- 석사학위를 취득한 후 7년 이상
- 정보 통신기사 · 정보처리기사 및 전자계산기조직응용기사 자격을 취득한 후 5년 이상 실무에 종사한 자
- ➔ + 3년 이상 개인정보의 보호 또는 데이터 이용과 관련한 경력이 있는 사람
- 개인정보의 가명·익명 처리 관련한 경력이 5년 이상인 사람

데이터 전문기관(신정법 기준)

데이터 결합 및 데이터 전문기관 요건

(법 제26조의4, 영 제 22조의 4)

데이터 결합

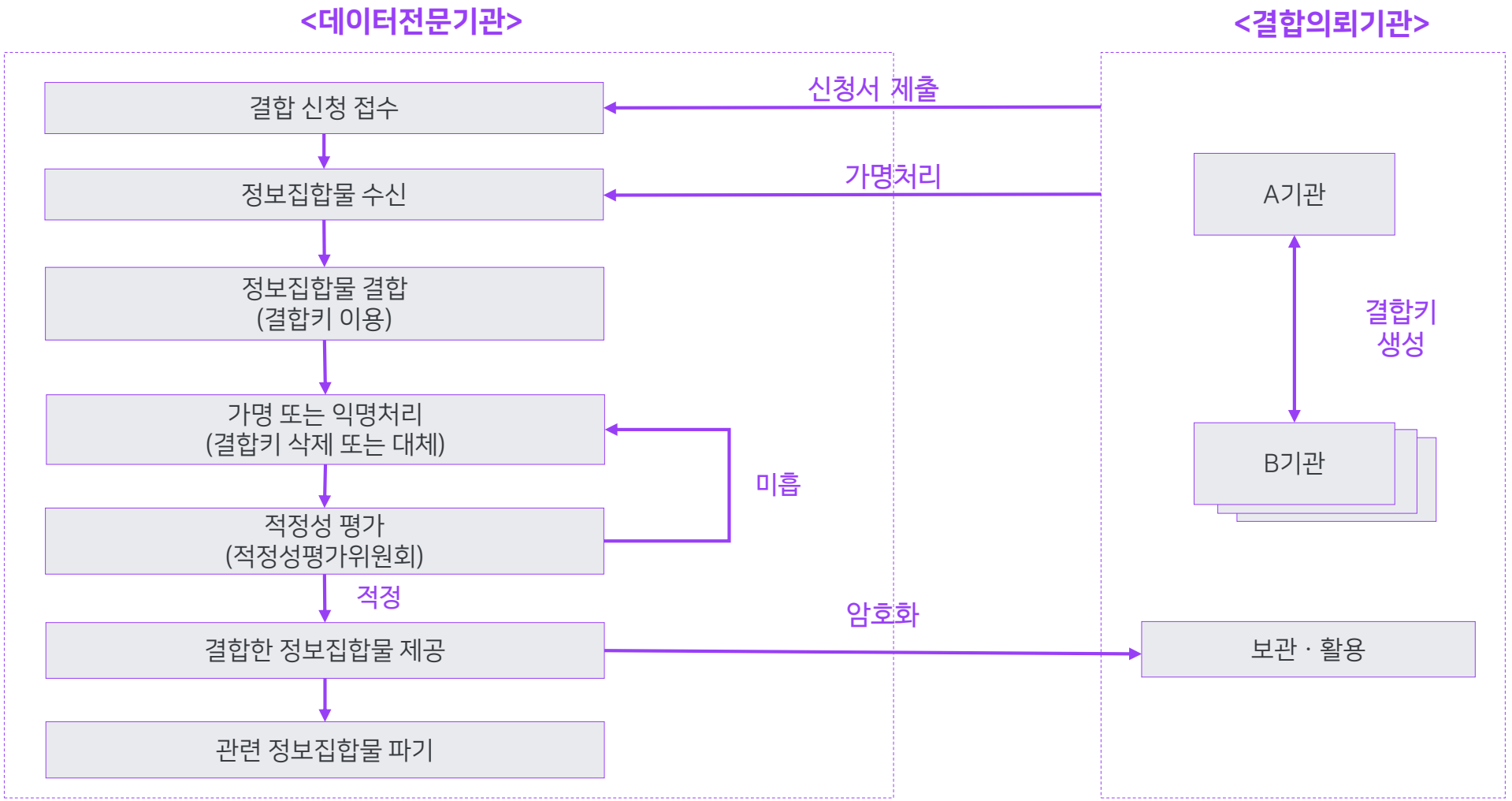
- 통계작성(시장조사 등 상업적 목적의 통계 작성을 포함(개보 법에는 없는 내용)), 연구(산업적 연구를 포함), 공익적 기록 보존을 위해서는 가명 정보를 신용정보주체의 동의 없이도 이용하거나 제공할 수 있도록 규정 (제32조제6항 제9의2, 제9의4)
- 가명 정보의 결합 및 익명 처리의 적정성 평가는 전문기관(신용 정보원, 금융 보안원)에서 수행하게 함으로써 이업종 간 데이터의 결합을 촉진(금융-비 금융 회사간 데이터 결합)(법 제26조의4)
- 개인신용정보 유출 시 징벌적 손해배상금을 3배에서 5배로 확대하는 등 형사 책임보다 과징금 형태의 경제적 제재를 통해 금융회사의 책임(의무)을 강화

데이터 전문기관 요건

- 데이터전문기관 자격요건
  - 민법상 비영리법인
  - 금융위원회가 정하여 고시하는 자본금, 매출액 등 요건을 갖춘 법인
  - 금융위원회가 정하여 고시하는 시설·설비 및 인력·조직, 재정능력을 갖춘 법인
  - 신용정보의 유출 등 방지를 위한 위험관리체계와 신용정보주체 권익 보호를 위한 내부통제장치 마련
- 데이터전문기관의 위험관리체계
  - 정보 집합물 간의 결합 업무를 수행하는 직원이 익명 처리에 대한 적정성 평가 업무를 동시에 수행하지 아니할 것
  - 전문기관업무를 수행하는 직원이 이 법 또는 다른 법령에 따른 다른 업무를 동시에 수행하지 아니할 것
  - 전문기관업무를 수행하는 서버와 다른 업무를 수행하는 서버를 별도로 분리할 것

정보집합물 결합 절차

(고시 제15조의2 제6항)



데이터 전문기관 지정요건

(고시 제28조의3)

시설 및 설비

가. 정보처리·정보통신설비

(1) 시스템 구성

1. 시스템 구성에 다음 항목을 포함할 것
   가. 정보집합물 결합 시스템
   나. 가명·익명처리 시스템
   다. 익명처리 적정성 심사 지원 시스템
   라. 보안서버 및 통신구간 암호화 시스템
2. 백업 및 복구시스템
3. 시스템 보안 및 시설 보안을 포함한 보안관리 체계

(2) 시스템 성능

1. 대용량 데이터를 결합하고 가명·익명처리 할 수 있는 성능을 갖출 것
2. 백업 및 복구작업이 최소한의 시간내에 가능할 것

(3) 보안체계

1. 방화벽과 침입탐지시스템을 갖출 것
2. 인터넷 구간의 네트워크와 데이터전문기관 업무 네트워크를 분리하여 운용할 것
3. 정보이용자 확인 체계(사용자 인증)를 갖출 것
4. 데이터 암호화처리 체계를 갖출 것
5. 외부침입 방지, 출입자관리 통제 및 데이터 반·출입 통제에 대한 대책을 강구할 것
6. 백업 및 소산관리 대책을 강구할 것

나. 업무공간과 사무장비

(1) 신용정보회사등으로부터 제공 받은 정보집합물을 안전하게 결합하고 가명 · 익명 처리하기 위한 전용 시스템 및 분리된 사무공간을 갖출 것

(2) 데이터전문기관 업무 수행 인원 대비 충분한 업무공간 및 사무장비를 갖출 것

(3) 내부기관 및 감독기관 등이 감독·검사업무를 수행함에 있어 법적 장애가 없을 것

다. 업무의 연속성을 유지할 수 있는 보완설비

(1) 파업 등 불시사태 또는 비상사태에 대비한 비상계획(Contingency Plan)이 마련되어 있을 것

인력 및 조직

다음의 어느 하나에 해당하는 인력을 8명 이상 상시 고용하고 데이터/보안 전문인력, 법률 전문인력 각각 최소 2명 이상 포함

(1) 데이터 및 보안 전문인력

- ✓ 기술사, 박사 학위를 취득한 자 + 2년 이상 관련 업무 수행
- ✓ 석사 학위를 취득한 자 + 4년 이상 관련 업무 수행
- ✓ 학사 학위를 취득한 자 + 6년 이상 관련 업무 수행
- ✓ 관련 분야에서 8년 이상 관련 업무 수행 경력 자

(2) 법률 전문인력

- ✓ 변호사 자격 소지자 + 1년 이상 관련 법률 업무 수행 경력
- ✓ 법학박사 학위 취득자 + 2년 이상 관련 법률 업무 수행 경력
- ✓ 법학석사 학위 취득자 + 4년 이상 관련 법률 업무 수행 경력
- ✓ 법학학사 학위 취득자 + 6년 이상 관련 법률 업무 수행 경력
- ✓ 8년 이상 관련 법률 업무를 수행한 경력자

관리체계

가. 신청인의 설립취지와 현재 영위하고 있는 사업영역이 데이터전문기관 업무 수행에 적합할 것

나. 데이터전문기관 업무 수행에 적합한 이해상충방지체계를 갖출 것

데이터 활용 유형별 법적 요구 및 준비사항

데이터 활용 형태별 법적 요구 및 준비 사항

활용 유형	법적 요구사항	기업별 준비사항
내부 데이터/내부 활용 (데이터 활용)	• 3대 목적내 가명 처리, 또는 익명 처리 활용 • 내부 결합 허용, 적정성 평가 후 활용 • 가명 정보/추가정보 보호 조치, 기록 유지	• 조직 및 활용 목적에 맞는 체계 사전 준비 • 비식별 처리, 결합, 평가, 키 관리 시스템 구축 • 기술적, 관리적, 물리적 보호조치 설계, 구축
내부 데이터/외부 제공 (데이터 판매)	• 3대 목적내 가명 처리 또는 익명 처리 • 외부 제공 적정성 평가 • 계약서내 보존기간, 보호의무, 파기 의무 명기	• 사전준비, 적정성 평가 체계 수립 • 비식별 처리, 평가 시스템 구축 • 데이터 가공 및 중계 서비스 연계, 보호조치 수립
외부 데이터/내부 활용 (데이터 구매)	• 가명 정보 보호조치, 주기적 적정성 평가 • 필요시 추가적인 가명/익명 처리 • 기간 만료 시 즉시 파기	• 데이터 평가 및 활용 체계 수립 • 가명화, 익명화 비식별 처리 시스템 구축 • 데이터 가공 및 중계 서비스 연계, 보호조치 수립
결합 신청 기관 (데이터 결합)	• 데이터 결합 전문기관 의무 활용 결합 • 결합 제공 전 가명 처리, 임시 대체 키 생성 • 추가적 가명/익명 처리, 적정성 평가 후 활용	• 데이터 결합, 활용 관리 체계 수립 • 사전/사후 비식별 및 평가 시스템 구축 • 데이터 가공 및 중계 서비스 연계
결합 전문기관 (결합 전문기관)	• 전문기관 지정기준 충족 지정신청/승인 • 가명 결합, 가명/익명 처리, 적정성 평가 수행 • 안전 전송, 보호조치, 기록관리, 정기적 보고	• 데이터 결합 전문기관 체계 수립 • 데이터 결합 전문 기관용 시스템 구축 • 업무 관리용 포털 구축(SI)

파수(Fasoo) 서비스

컨설팅 (ADS)

- 비식별 데이터 Risk 진단
- 비식별 조치 지원
- 비식별 방법론 제공
- 적정성 평가 대응
- 데이터 결합 전문기관 체계 수립
- 비식별화 전략 수립
- 기술적, 관리적 보호조치 방안 수립
- 신기술, 법제도 적용방안 수립

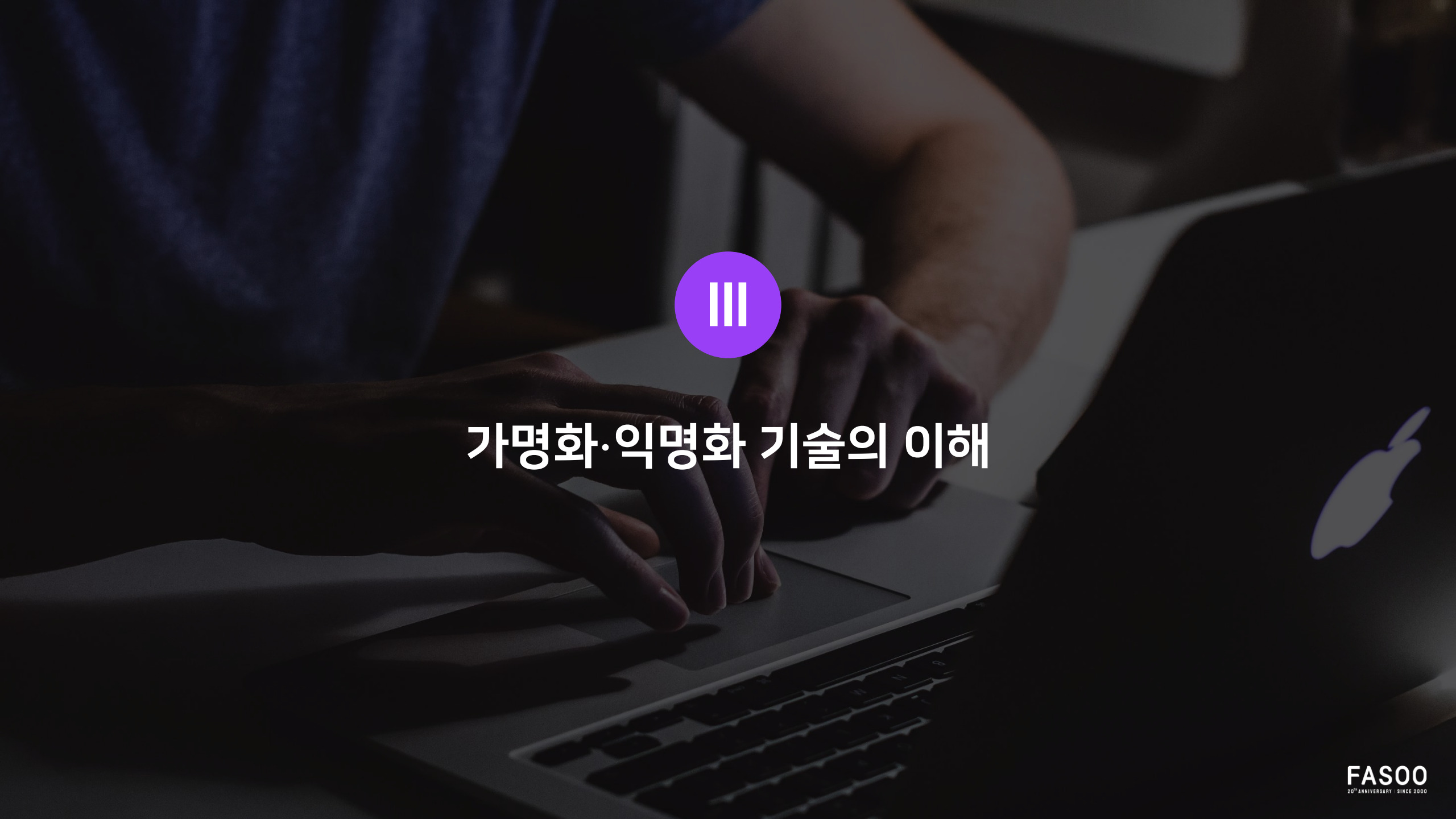
AnalyticDID

Analytic De-identification
Consulting Service

Analytic **De-identification**
Solution

솔루션 (AnalyticDID)

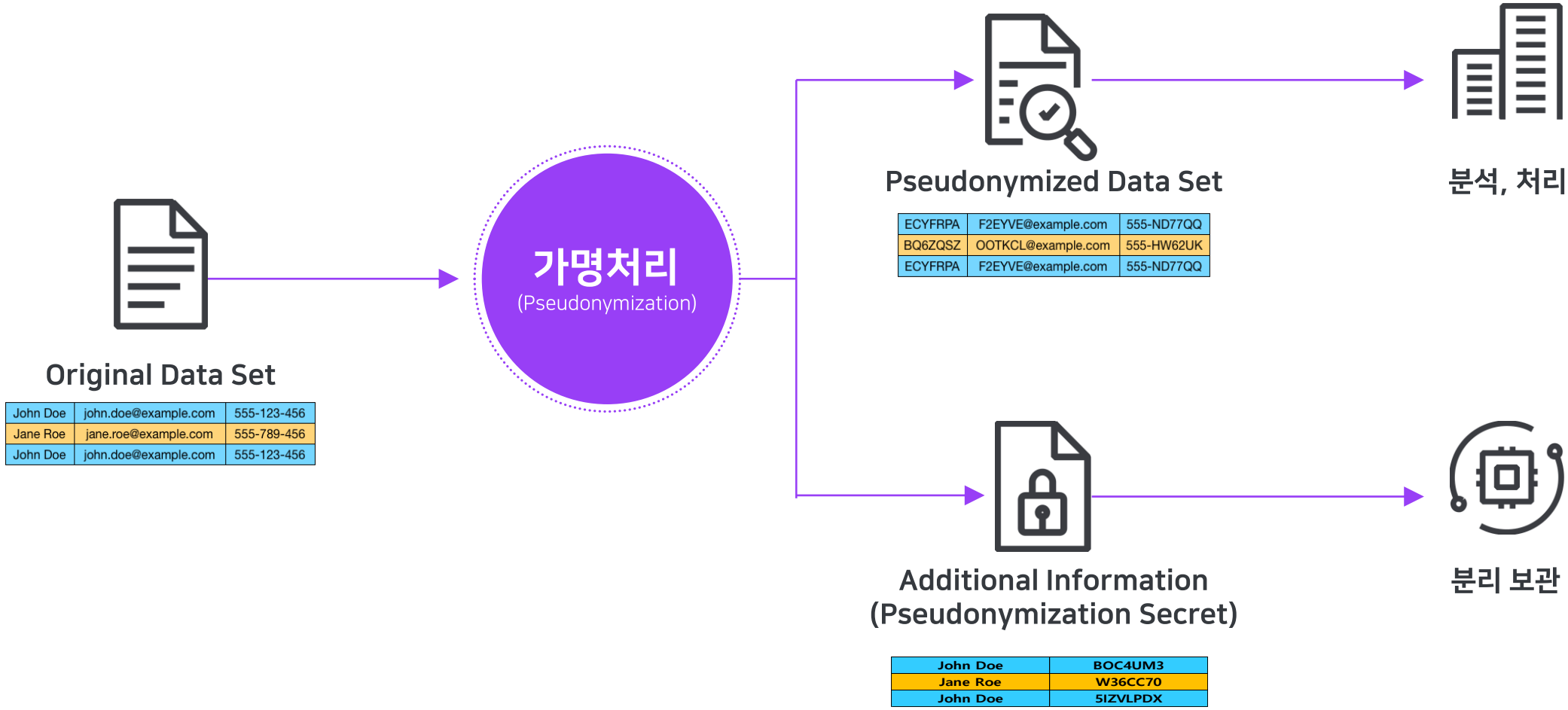
- 가명화, 익명화 플랫폼
- 데이터3법 및 가이드 100% 준용
- 데이터의 효용성 보장
- 맞춤형 (모듈형) 제품 라인업
- 데이터 전문기관 특화 솔루션 지원
- 비식별 작업 업무 프로세스 지원
- 최고의 속도와 용량 제공
- 업무 자동화 지원(옵션)



III

가명화·익명화 기술의 이해

가명화의 의미



가명화 기술(Pseudonymization Techniques)

주요 가명화 기술(Pseudonymization Tech)

가명화 기술	기능	장점	단점
Counter	• 가장 단순한 가명화 함수 • 중복없이 증가하거나 감소하는 연속된 숫자로 치환	• 쉽고 단순하여 작은 Data Set에 적합 • 식별자와도 전혀 연결관계를 갖지 않음	• 매핑테이블이 커져 복잡하고 큰 데이터셋에는 사용이 어려움
Random Number Generation (RNG)	• Counter와 비슷하나 id별로 랜덤번호가 할당됨 • 램덤번호 선택 확률은 전체 데이터 모수 기준 동일	• Counter보다 높은 식별자 보호 가능 • 매핑 테이블 없이 식별자 유추 불가	• 중복(Collision) 발생 가능 • 완벽한 랜덤번호 발생기 필요
Cryptographic hash function	• 가변 길이 데이터를 입력받아 고정 길이 문자열 반환	• 역변환 불가(One-way), Collision Free • 가명화 수준: 축약문(Digest) 길이에 의존	• 무결성에 기여도가 높지만 Brute Force, Dictionary 공격에 취약
Message Authentication Code (MAC)	• Keyed Hash Function으로 가명정보 생성시 Secret Key를 사용, HMAC은 인터넷에서 활발히 사용됨	• 가장 많이 사용하는 가명화 기술 • Key만 유출되지 않으면 안전	• 작은 변형에도 다른 Tool과 확장성이 요구되는 경우도 있음
Encryption	• 보통 비밀키 방식의 AES같은 블록 암호가 사용됨 • 블록사이즈에 따라 Padding 또는 축약 행위 추가	• 비밀키는 가명화, 복호화시 모두에 사용됨 • 다양한 속성자에 많이 사용되는 기술	• 식별자 크기가 크면 Mode Operation 사용 (초기화 벡터 필요)

출처 : Pseudonymisation techniques and best practices, enisa, November 2019

추가 정보(Pseudonymization Secret) 관리

✓ 추가정보 : 가명화 처리된 **데이터를 다시 원래의 데이터로 역 변환하기 위해 필요한 정보** 또는 데이터

✓ **보통 매핑 테이블(Mapping Table), Hash Algorithm, Hash Key, Encryption Key, Slat값** 등을 의미하며 **다음과 같이 관리**해야 함.
① 데이터 셋과 **분리 보관**, ② 메모리 저장소나 시스템 내에서 **완전 삭제**, ③ 허가된 관계자만 접근하도록 **완전한 접근제어 및 접속 기록 관리**
④ 컴퓨터에 저장된 경우 **암호화**를 하여야 하며 이 암호화 파일을 위한 적절한 키관리 및 저장소 관리가 필요함.

익명화 기술(Anonymization Techniques)

비식별 처리 기술

통계기술	• 데이터 추출(Sampling) • 데이터 총계처리(Aggregation)
암호기술	• 결정적 암호화(Deterministic encryption) • 순서보존 암호화(Order-preserving encryption) • 형태보존 암호화(Format-preserving encryption) • 동형암호(Homomorphic encryption) • 동형 비밀 분산(Homomorphic secret sharing)
범주화 기술	• 마스킹 (Masking) • 특정 속성값 삭제(Local suppression) • 레코드 삭제(Record suppression)
가명화 기술	• 매핑 테이블(Mapping table) • 단방향 암호화(Hash encryption)
해부화	• 해부화(Anatomization)
일반화 기술	• 라운딩(Rounding) • 상위및 하위 코딩(Top and bottom coding) • Combining a set of attributes into a single attribute • 로컬일반화(Local generalization)
무작위 기술	• 잡음추가(Noise addition) • 치환 (Permutation) • 부분집계(Micro aggregation)
데이터 합성 기술	• 합성데이터(Synthetic data)

프라이버시 보호 모델(적정성 평가)

1. K-익명성(K-anonymity)

모든 QI의 조합의 값이 동일한 행이 K개 이상으로 나타나도록 하여 개인의 식별 가능성을 낮추는 기법

나이	성별	주소	소득	
20	남자	대구	150만	
20	남자	대구	200만	→ K=3
20	남자	대구	200만	
30	여자	부산	180만	
30	여자	부산	180만	→ K=2
40	남자	서울	250만	

위의 표에서 위의 세줄은 K=3을 중간의 2줄은 K=2를 만족

2. L-다양성(L-diversity)

SA로 지정된 컬럼에 대해 L개 이상의 값을 가질 수 있도록 만드는 기법

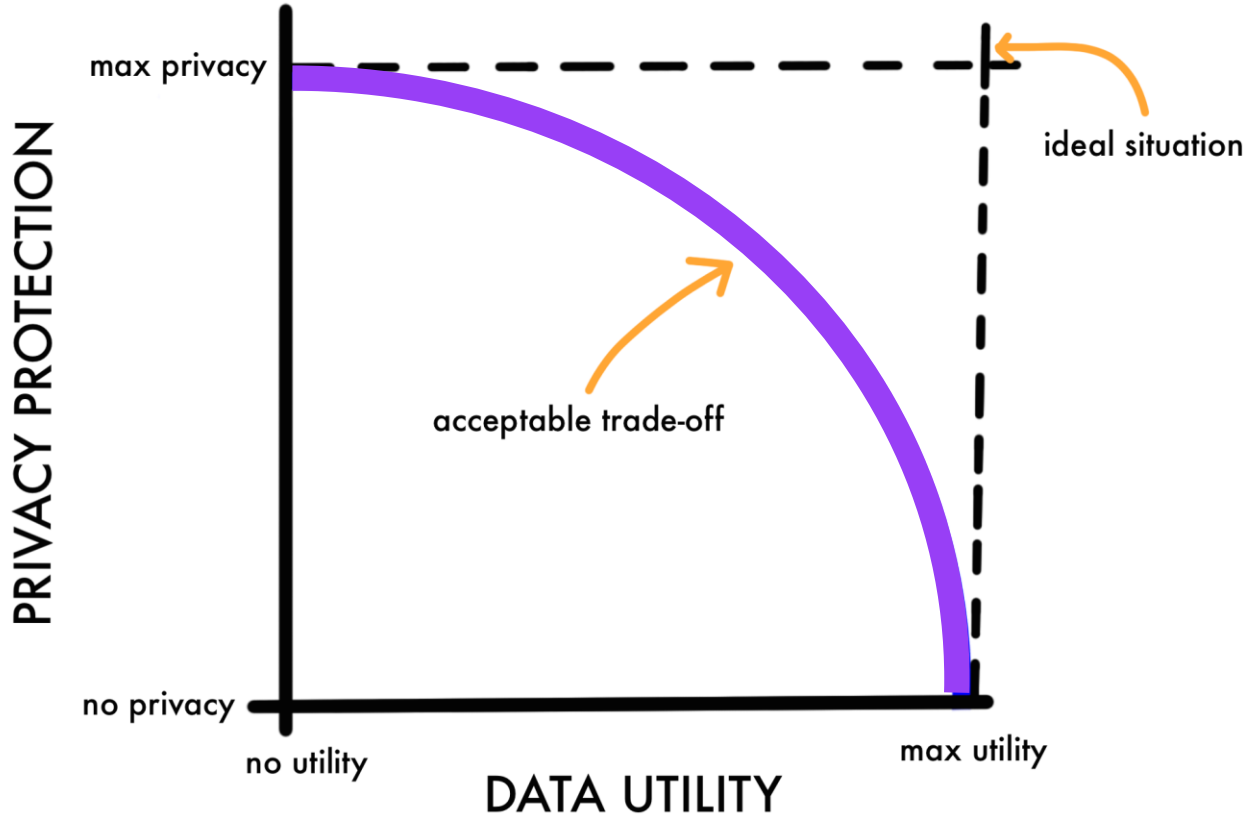
위의 세 줄은 소득값이 두 가지라 L=2를 만족하나 중간의 두 줄은 소득값이 동일하여 L=2를 만족 못함

3. t-근접성(t-closeness)

SA로 지정된 컬럼의 분포가 원데이터의 분포와유사한 분포를 가지도록 만드는 기법

가장 강력한 기법으로 일부 의료데이터에서만 사용

비식별 수준의 적절성



출처 : Practical Implications of Sharing Data: A Primer on Data Privacy, Anonymization, and De-Identification, 2015, Gregory S. Nelson, ThotWave Technologies, Chapel Hill, NC

올바른 비식별 처리

(목적에 맞는 비식별 처리)

재식별 위험 기준을 만족하면서 **사용목적에 따른** 연구가 가능한 **비식별 데이터 생성이 중요**

Original Data

이름	나이	성별	주소	소득
Daniel	23	남자	대구 중구	150만
Sean	25	남자	대구 서구	200만
Philip	27	남자	대구 북구	200만
Kate	32	여자	부산 동래구	180만
Helen	38	여자	부산 해운대구	180만
Jamie	46	남자	서울 마포구	250만

De-identification

1. 나이에 따른 소득을 연구하는 경우

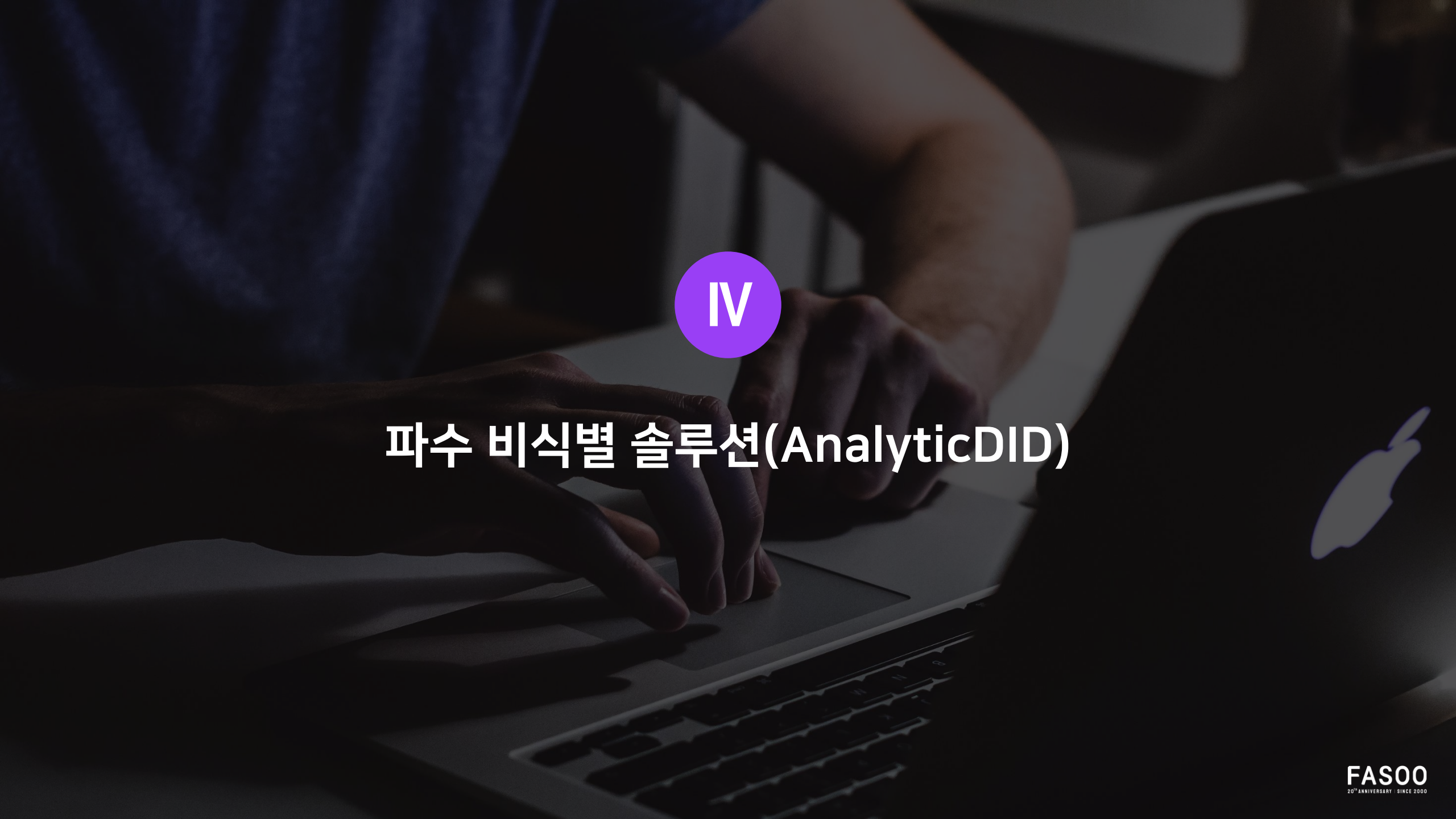
이름	나이	성별	주소	소득
*	20초반	*	대구	150만
*	20중반	*	대구	200만
*	20후반	*	대구	200만
*	30초반	*	부산	180만
*	30후반	*	부산	180만
*	40중반	*	서울	250만

- 식별자인 이름 데이터는 삭제
- 준식별자 중 사용 목적에 중요한 나이는 범주화 수준을 적게(초/중/후반으로 구분) 적용하여 나이에 대한 상세 정보 제공
- 단 성별과 주소에 대해서는 범주화 수준을 높게 적용하여 재식별 위험을 낮춤

2. 지역에 따른 소득을 연구하는 경우

이름	나이	성별	주소	소득
*	20대	*	대구 중구	150만
*	20대	*	대구 서구	200만
*	20대	*	대구 북구	200만
*	30대	*	부산 동래구	180만
*	30대	*	부산 해운대구	180만
*	40대	*	서울 마포구	250만

- 식별자인 이름 데이터는 삭제
- 준식별자 중 사용 목적에 중요한 주소는 비식별을 적용하지 않고 주소에 대한 상세 정보 제공
- 단 나이와 성별에 대해서는 범주화 수준을 높게 적용하여 재식별 위험을 낮춤



Ⅳ

파수 비식별 솔루션(AnalyticDID)

AnalyticDID 특징

Compliant

국내 데이터3법, 비식별조치 가이드라인 완벽지원
'Compliance Kit'을 통한 글로벌 컴플라이언스 자동설정
(ISO 20889, GDPR, CCPA 등)

Modularity

6개의 모듈형 제품 구성
: 전처리, Core, 평가, 결합, 키관리, 전송
필요에 따라 선택적 제품 구성 가능

Functions Outstanding Features

20여개의 다양한 가명화·익명화 기능 지원
국내최대 프라이버시 보호 모델(K,L,T외 총 8개 모델 제공)
최적 노드 분석 등 다양한 재식별 위험 분석 및 시각화 지원
5개 특허 보유, GS인증 취득, IAPP Tech Vendor 등록 예정

Reference

국내 최대 비식별 컨설팅 수행
: 보건복지부, 국민건강보험공단, KISA, NIA 등
다수 전문기관에서 ADID 선택
: 금보원, NIA, KISA, SISS, KERIS, KDATA 등
기타 20여개 공공, 금융, 민간에서 제품 사용 중

모듈별 기능 및 특징

시스템	기능 / 특징
Analytic DID	• 가명화/익명화 비식별 기법 지원 • 4대 식별정보, 전화 번호 등 민감 정보 검출, 처리 기능 • Spark 기반의 대용량 처리 지원 • 비식별 조치 완료 후 Raw 데이터 완전 삭제 가능
Analytic DID Assessment	• 비식별된 결과를 분석하여 비식별에 대한 위험 수치를 제공하는 시스템 • 재식별 리스크와 비식별 데이터의 유용성을 판단할 수 있음
Analytic DID ETL	• RDBMS 연계 또는 일반 파일(csv, txt)에서 데이터 추출 기능 • 데이터 정제 기능
Analytic DID Mergence	• 결합, 적정성 평가를 하나의 시스템으로 구성함 • 결합된 데이터의 민감 정보 검출 기능
Analytic DID KMS	• 연계 키 생성/관리/완전 삭제 기능 • 유효기간 설정을 통한 관리 기능
Analytic DID Transfer	• 대용량 데이터의 전송을 위한 데이터 압축/이어받기/무결성 검증 지원 • 파일의 안전한 제공을 위한 데이터 암호화 기능 제공

AnalyticDID Core

AnalyticDID
De-identification Solution for Analytics

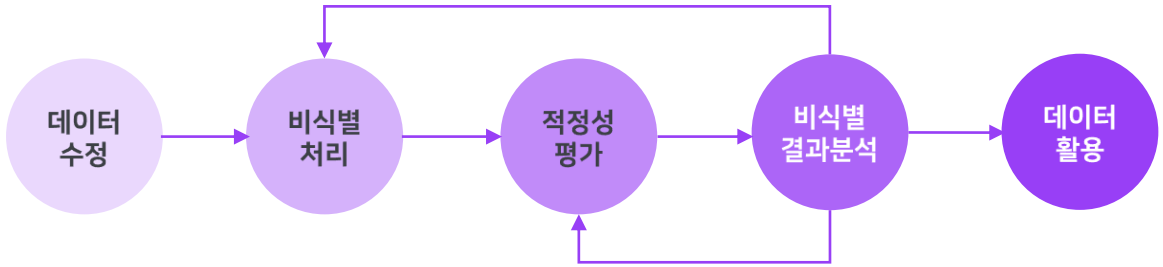
"기계적인 비식별화가 아닌 효용성이 있는 비식별 데이터를 제공하면서 법적 기준을 완벽하게 지원하는 비식별화 전문 솔루션"

- 사용목적에 맞는 데이터 제공
- 쉽고 빠른 비식별 처리 가능
- 데이터 분석/비식별 처리 비용 절감

주요 특징

- 비식별화 자동화 플랫폼
- 최고의 속도와 용량 제공
- 데이터 효용성 보장
- 맞춤형 제품 라인업
- 비식별 작업 업무 프로세스 지원
- 비식별조치 가이드, ISO 20889 지원

비식별 프로세스



- 개인정보 검출
- Data 기반 필요 항목 설정

- 가이드라인 기반 비식별 기술 및 ISO/IEC 20889·2018 기반의 기술 적용

- K익명성, L다양성, T근접성, DP 등의 프라이버시 모델 지원

- 데이터의 위험/효용성에 대한 지표
- 다양한 시각화 기능을 통한 확인

- 최종 데이터의 개인 정보 검출
- 처리 완료 파일의 다운로드

AnalyticDID Assess

Analytic DID Assess
Detecting personal information &
Usability / Risk Measurement Solution

"기계적인 비식별화가 아닌 효용성이 있는 비식별 데이터를 제공하면서 법적 기준을 완벽하게 지원하는 비식별화 전문 솔루션"

개인정보
검출 및 제거

원 데이터와의
분포 특성 비교를 통한
유용성 측정

프라이버시
보호 모델 및
유사도 측정을 통한
개인식별 위험 측정

주요 특징

- 비식별화 자동화 플랫폼
- 최고의 속도와 용량 제공
- 데이터 효용성 보장
- 맞춤형 제품 라인업
- 비식별 작업 업무 프로세스 지원
- 비식별조치 가이드, ISO 20889 지원

솔루션 기능

개인정보 검출	• 개인정보(정규 표현식 & 정합성 모듈) 검출 • 검출 개인정보 제거
지표 측정	• 데이터 범주화에 따른 데이터 Lose 등 다양한 유용성 지표 제공 • 데이터 유사도, K-익명성 기반 재식별 위험도 등 다양한 개인식별 리스크 지표 제공
지표 관리	• 작업별 유용성/위험도 지표 한계 값 설정 기능 • 다양한 프라이버시 모델에 대한 지표 측정 및 관리

FASOO
20TH ANNIVERSARY | SINCE 2000

AnalyticDID ETL

Analytic DID ETL
De-identification ETL Solution

"다양한 환경에 저장되어 있는 데이터를 비식별에 적합하도록 추출, 정제, 변환 하는 솔루션"

다양한
Data Resource 지원

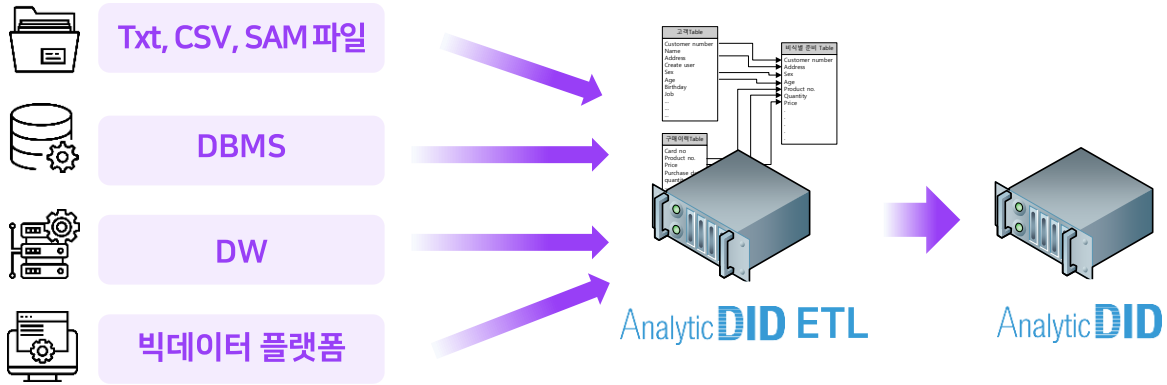
선택한
Privacy Model에
적합한 데이터 변환

정형뿐 아니라
비정형 (의료 영상 등)
데이터에 대한 변환 지원

주요 특징

- File, DB, DW, Hadoop 등 다양한 Resource 지원
- Data Type 변환
- Outlier 처리
- Null 처리 및 이상 Data 처리
- 컬럼별 추출 및 변환 처리
- 비식별을 위한 사전 처리 지원

ETL 프로세스



- 다양한 리소스의 다양한 Data를 비식별에 적합하도록 추출(지속적 추출을 위한 Batch Job 지원)
- 데이터 정제/가공 기능을 통해 Null, 오류값 등 이상 Data처리하여 비식별 솔루션으로 전송

AnalyticDID Mergence

Analytic DID Mergence
Data combination and convergence Solution

"대용량 데이터에 대한 다양한 형태의 결합과
결합된 데이터의 개인 식별 Risk에 대한
검사 기능을 제공하는 데이터 결합/융합 전문 솔루션"

결합 전
결합률 측정

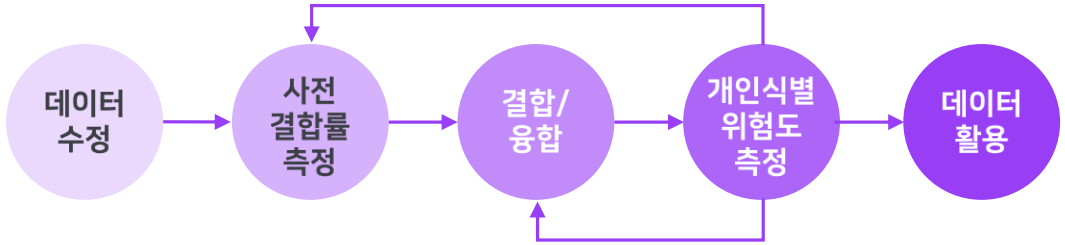
결합 데이터의
개인 식별 위험 제거

데이터의
신규 가치 창출

주요 특징

- 대용량 데이터 결합 지원
- 다양한 결합 방식 지원
- 결합데이터의 위험도 검사
- 맞춤형 제품 라인업
- 라인 단위, 세그먼트 단위 융합

결합 프로세스



- 연계/결합 데이터 분석
- 융합 기준 설정
- 결합 시 결합 키 컬럼 지정

- 결합 시 사전 결합률 측정을 통한 자원 낭비 최소화

- Left, Right, Full, Inner Join 등 다양한 결합 방식 지원
- 세그먼트 별 융합지원

- 결합된 데이터의 대한 개인식별 위험도 측정
- K,L,T 등 다양한 프라이버시 보호모델 기반 위험성 측정

- 최종 결합 데이터의 다운로드
- 다운로드 후 기존 데이터에 대한 완전삭제 기능 제공(DoD 기반 완전 삭제)

AnalyticDID KMS

AnalyticDID KMS
Key Management Solution (Indexer)

"영국의 ADRN 방식의
키 관리 기능이 적용된 안전한 연계,
결합을 위한 키 관리 솔루션"

연계, 결합의 안전성 강화

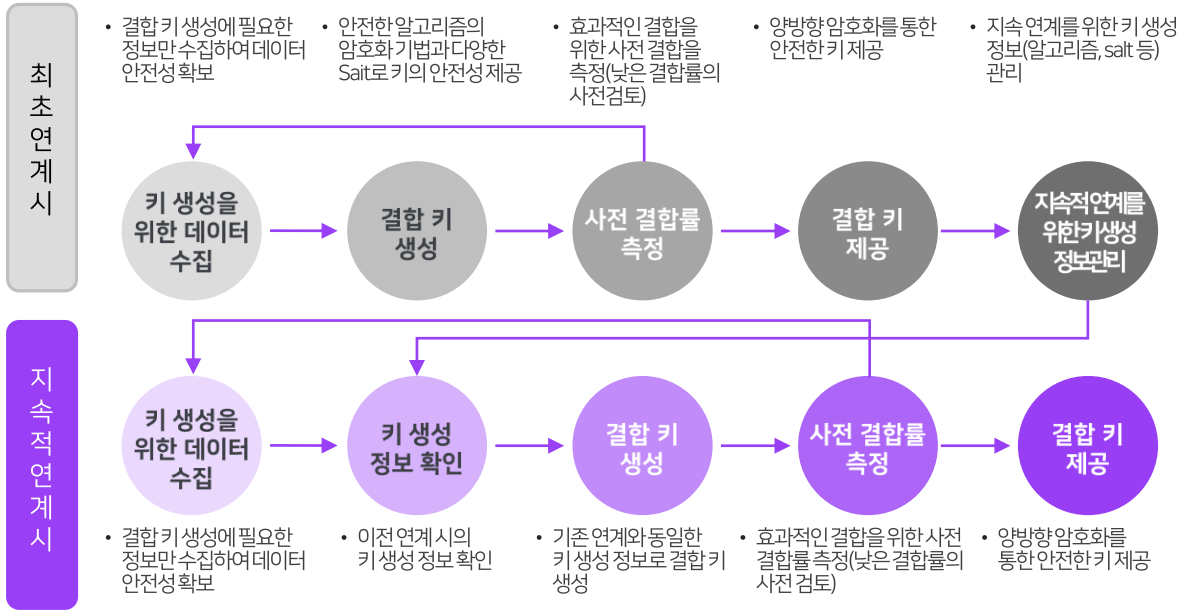
지속적 연계를 위한 키관리

ADRN의 Indexer 기능

주요 특징

- 결합 / 연계 키 관리 플랫폼
- 다양한 키 생성 알고리즘 지원
- 지속적 연계를 위한 키 관리 기능
- ADRN의 Indexer의 기능 제공
- 사전 결합률 측정을 통한 결합 효용성 증대

키 관리 프로세스



FASOO
20TH ANNIVERSARY | SINCE 2000

AnalyticDID Transfer

Analytic DID Transfer
Big Data Secure Transmission Solution

"대용량 빅데이터의 안전하고 정확한 전송을 지원하는 데이터 전송 솔루션"

- 국정원 인증 암호화 모듈 사용
- 압축 및 분할 전송을 통한 빠르고 안전한 전송
- 무결성 검증, 바이러스 검사를 통한 안전한 사용 지원

주요 특징

- 대용량 데이터를 위한 CS 구조
- 전송 데이터 무결성 검증
- 데이터 수신 후 바이러스 검사를 통한 안전한 사용
- 오류에 대한 검사 및 재전송 기능
- 이어받기 기능으로 다양한 오류 상황에 대비

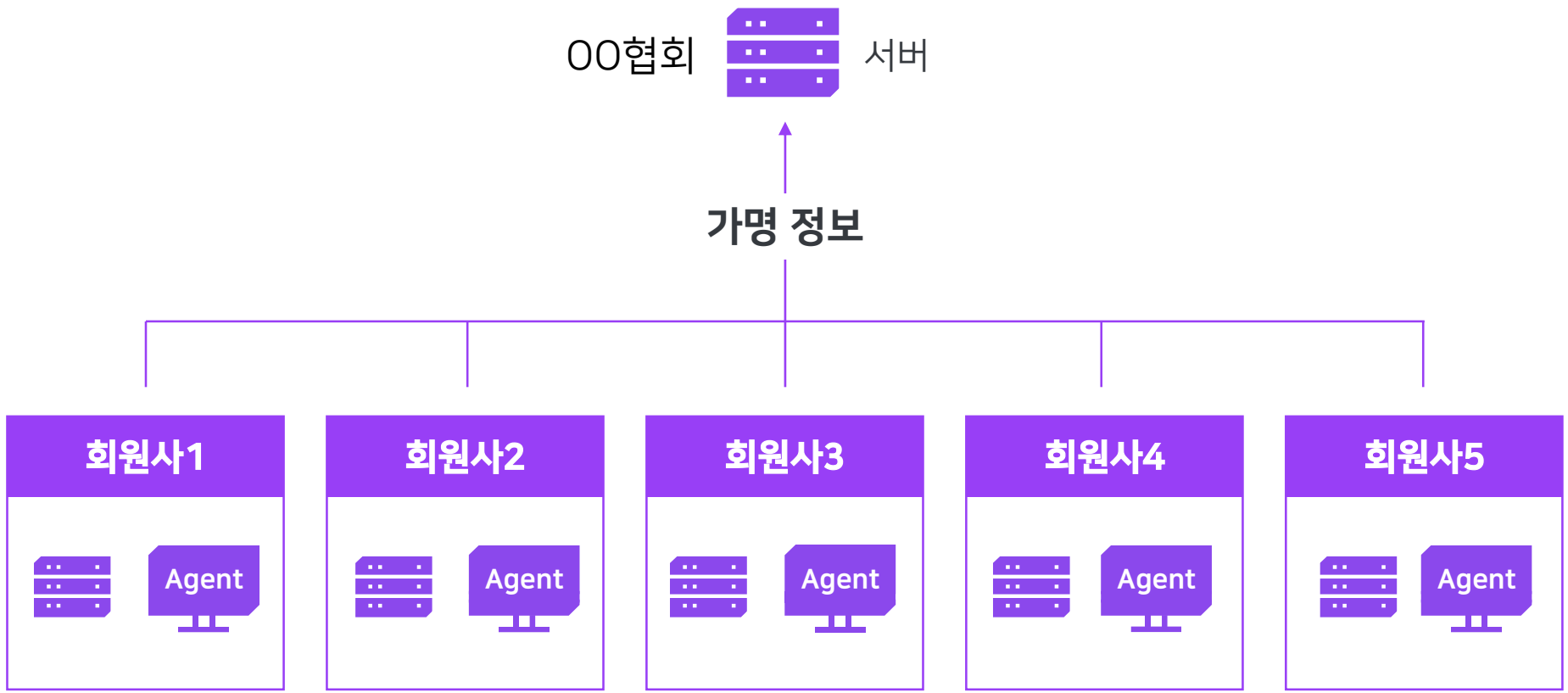
파일 전송 프로세스

AnalyticDID 적용사례

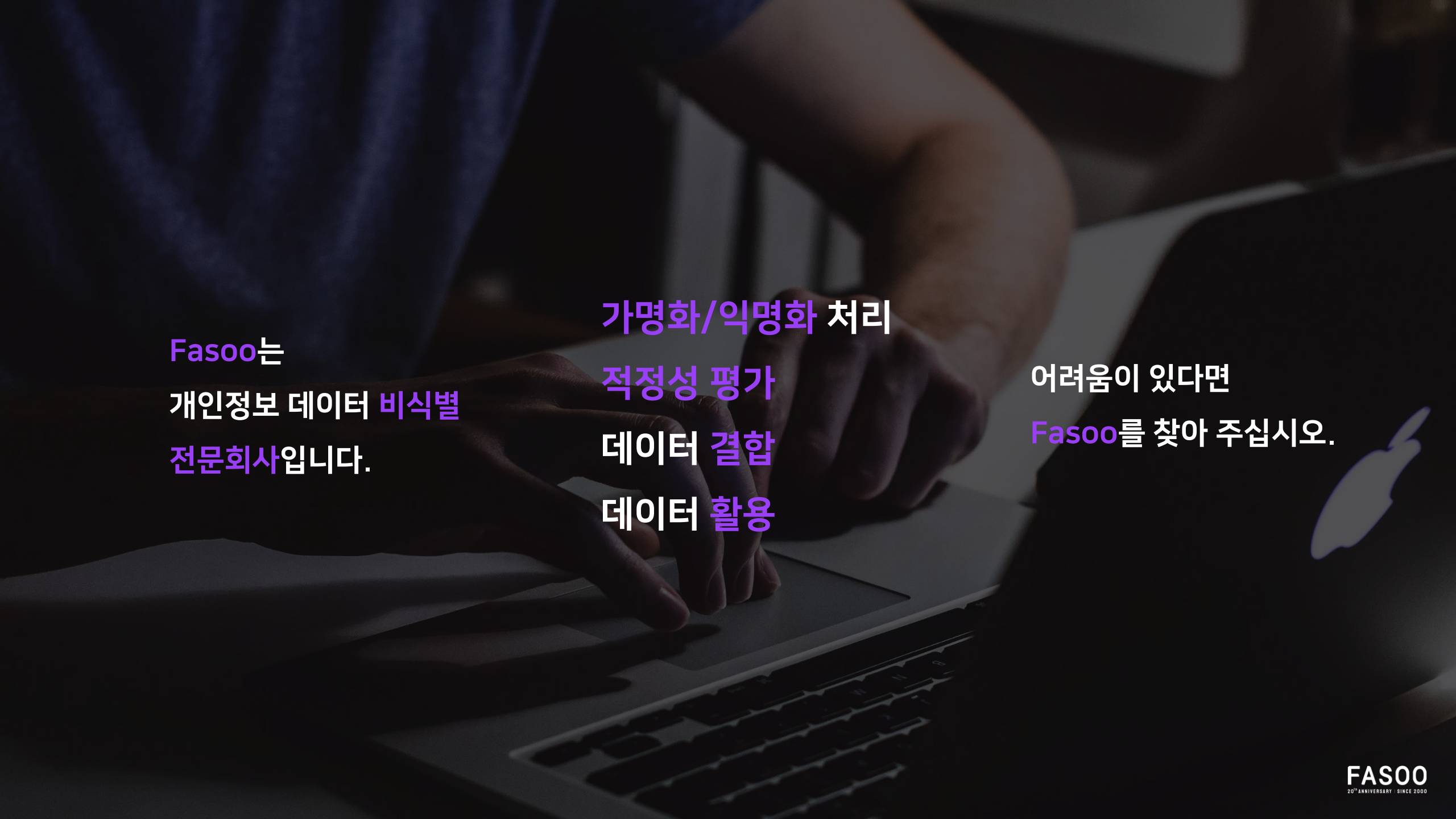
FASOO
20TH ANNIVERSARY | SINCE 2000

빅데이터 플랫폼 및 센터 모델

Agent 기반 가명 정보 수집 모델



DB로부터 개인정보를
받아서 가명처리



Fasoo는
개인정보 데이터 비식별
전문회사입니다.

가명화/익명화 처리
적정성 평가
데이터 결합
데이터 활용

어려움이 있다면
Fasoo를 찾아 주십시오.

FASOO
20TH ANNIVERSARY | SINCE 2000