CPO 핸드북

개 인 정 보 보 호 책 임 자

개인정보보호위원회
Personal Information Protection Commission

KCPO 한국개인정보보호책임자협의회
Korean Chief Privacy Officers Council

CHIEF PRIVACY OFFICERS

목 차

I

발간취지

Ⅰ 발간취지

- CPO핸드북은 개인정보 보호·활용에 필요한 법적 의무를 이행함에 있어, CPO가 고려해야 할 사항과 대응 방안에 대한 이해를 돕기 위함
  - CPO의 역할과 업무는 기업·기관의 규모 및 조직형태, 산업 분야·사업부문 등에 따라 상이할 수 있으므로 동 핸드북의 탄력적인 활용 필요

    ※ 동 핸드북은 법적 효력이 없으며, 관계 법령 우선 적용 필요

- 향후, 한국CPO협의회를 중심으로 조직 및 산업별 개인정보의 특성을 고려하여 동 핸드북을 지속적으로 확대 · 발전시켜 나갈 예정

- 동 핸드북에서 사용하는 주요 용어 및 약칭은 아래와 같음

| 주요 용어 및 약칭 |

용 어	약 칭
개인정보 보호책임자	CPO (Chief Privacy Officer)
정보보호 최고책임자	CISO (Chief Information Security Officer)
개인정보 보호법	법
개인정보 보호법 시행령	영
개인정보보호위원회	개인정보위
한국인터넷진흥원	KISA

Ⅱ

개인정보 보호책임자 (CPO) 제도

Ⅱ 개인정보 보호책임자(CPO) 제도

1 CPO 정의 및 역할

◆ CPO의 의의

- CPO 제도는 개인정보 관련 법규 준수, 오남용 방지 등 개인정보처리자의 개인정보 보호 활동을 촉진하고 책임을 부과하는 규제 장치
  - (CPO의 정의) 보호법상 CPO는 개인정보 처리에 관한 업무를 총괄하여 책임지는 자를 의미
  - (CPO 지정 의무) 개인정보처리자는 CPO를 지정해야 함(소상공인 제외)

법(제31조)·시행령(제32조)

제31조(개인정보 보호책임자의 지정 등) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다. 다만, 종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자의 경우에는 지정하지 아니할 수 있다. 〈개정 2023. 3. 14.〉

② 제1항 단서에 따라 개인정보 보호책임자를 지정하지 아니하는 경우에는 개인정보처리자의 사업주 또는 대표자가 개인정보 보호책임자가 된다. 〈신설 2023. 3. 14.〉

시행령 제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제1항 단서에서 "종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 「소상공인기본법」 제2조제1항에 따른 소상공인에 해당하는 개인정보처리자를 말한다. 〈신설 2024. 3. 12.〉

주요 업무 및 역할

- 법령에서 규율하고 있는 CPO의 주요 업무는 아래와 같음

  ① 개인정보 보호 계획의 수립 및 시행

  ② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

  ③ 개인정보 처리와 관련한 불만의 처리 및 피해 구제

  ④ 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제시스템의 구축

  ⑤ 개인정보 보호 교육 계획의 수립 및 시행

  ⑥ 개인정보파일의 보호 및 관리 · 감독

  ⑦ 법 제30조에 따른 개인정보 처리방침의 수립 · 변경 및 시행

  ⑧ 개인정보 처리와 관련된 인적 · 물적 자원 및 정보의 관리

  ⑨ 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기

  ⑩ 기타 개인정보 등 관련 법령에서 명시하는 사항

- 개인정보 보호 계획의 수립부터 주기적 관리 · 감독까지 개인정보 보호 · 활용과 관련된 전반적 관리 업무를 수행
  - CPO는 개인정보 정책을 지속적으로 현행화하고 개인정보 생애주기 모든 단계를 관리 · 감독할 의무를 가짐
  - 법령에서는 CPO 업무에 대한 의무사항을 중심으로 최소한으로 규정하고 있으므로, CPO는 최신 개인정보 보호 이슈, 법제도 제 · 개정 사항 등 대내외 환경을 고려하여 업무 및 역할 수행 필요

2 CPO 직위 및 자격요건

직위요건

- (도입 취지) 개인정보 보호와 관련하여 필요한 인력, 예산 등 자원을 할당할 수 있도록 일정 직급 이상(C-level)의 CPO 지정 필요
- (공공기관) 최소 4급 이상 공무원 또는 개인정보 처리 관련 업무를 담당하는 부서의 장으로 지정 (시행령 제32조제3항제1호)
- (공공기관 이외) 사업주 또는 대표자나 임원으로 지정(시행령 제32조제3항제2호)
  - 임원이 없는 경우* 개인정보 처리 관련 업무를 담당하는 부서의 장
    * "개인정보 처리 관련 업무를 담당하는 임원이 없는 경우" 또는 "자격요건을 충족하는 임원이 없는 경우"가 아닌 전체 조직 내에 임원 직급을 가진 자가 없는 경우를 의미함

자격요건

- (도입 취지) 대량의 개인정보를 처리하는 개인정보처리자는 대내외적으로 일정한 수준의 개인정보 보호 업무 수행 필요
- (적용 대상) 연간 매출액, 보유하고 있는 개인정보 규모 등을 고려하여,
  - 일정 기준(시행령 제32조제4항의 각호)에 해당하는 개인정보처리자는 개인정보보호 경력 등 자격요건을 갖춘 자를 CPO로 지정 필요

자격요건 적용 대상

① 연간 매출액 또는 수입이 1,500억원 이상인 자로서
  1) 5만명 이상의 민감 · 고유식별정보를 처리하거나
  2) 100만명 이상의 개인정보를 처리하는 자
② 직전 연도 12월 31일 기준 재학생 수(대학원 재학생 수를 포함)가 2만명 이상인 「고등교육법」 제2조에 따른 학교
③ 「의료법」 제3조의4에 따른 상급종합병원
④ 공공시스템운영기관

- (자격 기준) 최소 2년 이상의 개인정보 보호 경력을 포함하여 개인정보 보호, 정보보호, 정보기술 경력을 합하여 총 4년 이상의 경력 보유
  - 각각의 경력을 모두 보유해야 하는 것은 아니며, 4년 이상의 개인정보 보호 경력만 보유한 경우도 자격요건 충족
  - 그 밖에 경력인정 가능 요건
    ① 개인정보 보호, 정보보호, 정보기술 관련 학위를 취득한 경우
    ② 유관 분야에서 자격인증 및 취득한 경우
    ③ 개인정보위가 주관하는 교육을 이수한 경우(최대 3개월)

| 개인정보 보호책임자 경력 인정 요건 |

구 분		경력 인정 요건	인정기간
시행령 [별표 1]	개인정보 보호 경력	· 개인정보 보호 관련 박사학위 취득자	2년
		· 개인정보 보호 관련 석사학위 취득자	1년
		· 개인정보 보호 관련 학사학위 취득자	6개월
	정보보호 경력	· 정보보호 관련 박사학위 취득자	2년
		· 정보보호 관련 석사학위 취득자	1년
		· 정보보호 관련 학사학위 취득자	6개월
	정보기술 경력	· 정보기술 관련 박사학위 취득자	2년
		· 정보기술 관련 석사학위 취득자	1년
		· 정보기술 관련 학사학위 취득자	6개월
고시 [별표 1]	개인정보 보호 경력	· 정보보호 및 개인정보 보호 관리체계 인증 등에 관한 고시 제14조에 따른 정보보호 및 개인정보 보호 관리체계 인증심사원 · 개인정보 영향평가에 관한 고시 제5조제2항에 따른 개인정보 영향평가 전문인력 ·「변호사법」 제4조에 따른 변호사 자격 취득자	1년
	정보보호, 정보기술 경력	· 정보관리기술사, 컴퓨터시스템응용기술사	1년
		· 정보보안기사, 정보처리기사	6개월

※ 각각의 인정 요건을 갖춘 경우, 구분된 경력(개인정보보호, 정보보호, 정보기술) 내에서는 하나의 요건만 인정하며, 구분된 경력별로는 중복인정 가능함

※「개인정보 보호책임자 경력 인정에 관한 고시」에 따라 개인정보위가 주관하는 교육을 이수하는 경우에는 고시 발령일 4년 전 교육부터 최대 3개월의 범위 내에서 개인정보 보호 경력을 인정

- (적용 시행일) 2024년 3월 15일부터 시행 중이나, 공공시스템운영기관 및 시행일 당시 종전 기준에 따라 CPO를 지정한 개인정보처리자는 적용 유예
  - (공공시스템운영기관) 2024년 9월 15일부터 시행되며, 자격요건 적용 대상인 경우 2년 이내('26.9.14.까지) 자격요건을 갖춘 자를 CPO로 지정 필요
  - (종전 기준에 따라 기 지정한 경우) 영 시행 후 2년 이내('26.3.14.까지) CPO 자격요건 충족 필요

3 CPO 독립성

◆ 독립성 보장

- (필요성) 기업의 비즈니스 활동 시 경영진의 합리적 의사결정 유도를 위한 개인정보 처리 업무 개선, 개인정보 유출 · 침해사고의 예방과 대응 등을 통해 기업의 위험(risk) 관리 필요
  - CPO가 개인정보 처리에 관한 총괄책임자로서 실질적 역할을 수행할 수 있도록 보장하고, 조직 내 개인정보 관련 사항에 대해 최고경영진부터 전사적으로 관심을 갖도록 하는 것이 바람직

- (독립성 보장 의무) 개인정보처리자는 CPO가 업무를 독립적으로 수행할 수 있도록 보장해야할 의무를 가짐(법 제31조제6항)
  - 시행령 제32조의 개정을 통해 아래와 같이 개인정보처리자에게 CPO의 독립적 업무 수행을 보장하도록 의무화
    ① 개인정보 처리와 관련된 정보에 대한 CPO의 접근 보장
    ② CPO가 개인정보 보호 계획의 수립 · 시행 및 그 결과에 관하여 정기적으로(연 1회 이상) 대표자 또는 이사회에 직접 보고*할 수 있는 체계의 구축
    * 기업 내 전사적인 관심을 유도하기 위해서는 이사회 보고가 바람직
    ③ 개인정보 보호책임자의 업무 수행에 적합한 조직체계의 마련 및 인적 · 물적 자원의 제공

Ⅲ

개인정보 보호책임자 (CPO) 업무

Ⅲ 개인정보 보호책임자(CPO) 업무

1 개인정보 거버넌스 구축 및 운영

1-1 개인정보 거버넌스와 개인정보 조직 체계

• CPO는 경영진의 지원을 기반으로 전사적인 개인정보 보호 활동의 효율적 추진을 위해 조직 구성, 협업 및 보고 체계 마련 등 개인정보 거버넌스를 구축하여야 함

개인정보 거버넌스 정의[1]

○ (거버넌스) 통상적인 통치(Government)가 아닌 다양한 이해 관계자들의 파트너십에 의한 협치(協治)를 의미하며 다양한 분야에서 논의

거버넌스(Governance)의 의미

✓ (기업 거버넌스) 주주, 종업원, 거래 기업, 지역사회 등 회사 관련 이해관계자들의 이해를 조정하여 의사결정, 결정된 사항의 집행 및 감시 감독

✓ (IT 거버넌스) IT 자원과 정보, 조직을 기업의 경영 전략 및 목표와 연계해 경쟁 우위를 확보할 수 있도록 하는 의사결정 및 책임에 관한 프레임 워크[2]

✓ (정보보호 거버넌스, ISO/IEC 27014) 정보보호에 대한 최고 경영진의 의사결정 권한과 책임, 비즈니스와의 전략적 연계, 컴플라이언스 보장을 위해 지켜야 할 원칙과 수행해야 할 활동 및 과제를 정의한 문서

✓ (디지털 거버넌스) 디지털 기술과 관련된 사회기술, 전략 및 규제 영역에 대한 조직의 접근 방식에 대한 역할, 책임 및 책임을 설정하는 구조와 프레임워크를 의미[3]

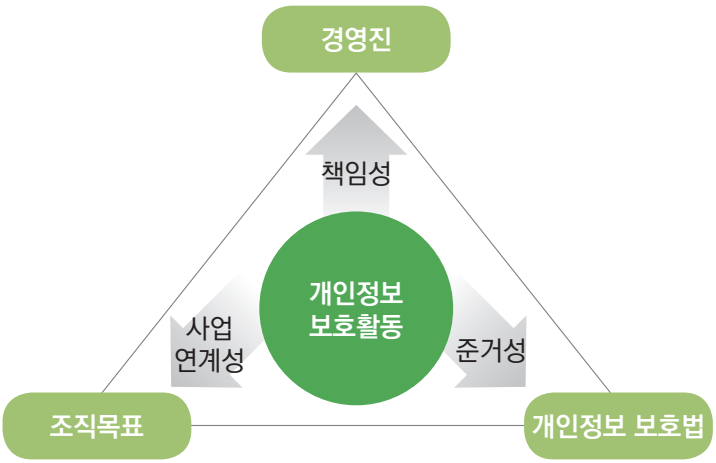
1) 금융보안원 금융보안 거버넌스 가이드(2019), IT 거버넌스 및 정보보호 거버넌스 관련 선행연구 등을 기반으로 재구성
2) 출처 : 한국정보통신기술협회(TTA) 정보통신용어사전
3) 출처 : Organizational Digital Governance Report 2024, IAPP

- (개인정보 거버넌스) 조직 전반의 개인정보 보호 및 활용 관련 전략과 정책을 수립하고 이행함에 있어 요구되는 의사결정 체계, 인적·물적 자원의 통제 수단과 방식 또는 관리 체계를 의미
  - 조직의 이익과 정보주체 권리를 보장하고 개인정보 보호와 활용 관련 전사적 전략과 정책의 수립 · 이행을 촉진하기 위한 최고 경영진 및 핵심 이해관계자의 역할과 책임으로 정의

개인정보 거버넌스 구축

- (고려 사항) 사업 연계성, 준거성, 책임성 등
  - 개인정보 보호 활동을 중심으로 조직의 성과 목표·전략 등 사업과의 연계성(Business Alignment), 관련 법령상의 의무 준수를 위한 준거성(Compliance), 경영진 및 개인정보취급자 등 이해관계자 대상 활동 결과에 대한 책임성(Accountability) 등을 종합적으로 고려하여 구축

| 개인정보 거버넌스 구축 시 고려 사항 |



  - (구성요소 및 범위) 경영진과 개인정보 보호 실무조직, 연관조직 간의 상호 협력을 통한 개인정보 보호 활동 중심으로 구성
    · 이를 위한 의제와 목표 결정, 사업 계획의 수립 및 이행, 인적·물적 자원의 할당, 이해관계 조정, 업무에 대한 평가 방안 등을 포함

핵심 이해관계자와의 협업

- (핵심 이해관계자 선정) 전사적 개인정보보호 활동을 위해 조직 내의 다양한 이해관계자 중 협업 대상인 핵심 이해관계자 선정 필요
  - 핵심 이해관계자를 선정하고 이해관계자별 역할을 명확히 정의하여 관련된 권한과 책임을 부여하기 위해 경영진 승인 필요

| 개인정보 거버넌스 구축을 위한 핵심 이해관계자의 역할 예시 |

핵심 이해관계자	주요 역할
CEO	· 개인정보 거버넌스 체계의 승인 · 개인정보보호 조직의 구성 보장 · CPO 지정 및 독립성 보장 · 경영진의 소통 지원 · CPO의 정기 보고
CPO	· 개인정보 거버넌스 체계 구축 · 개인정보 보호 조직의 구성 및 운영 · 개인정보 관리계획의 수립 및 이행 · 개인정보보호위원회의 위원장 역할 수행 · 경영진과의 소통을 통해 전사 개인정보 보호 활동 지원
CIO	· 원활한 IT 활동을 통한 경영진과의 소통 강화 · 비즈니스를 고려한 현재와 미래의 IT 목표 제시 · 개인정보보호 정책 등을 IT(운영 및 개발) 부서에 지시 · IT 정책을 수행하는 IT 부서 관리 감독 · CIO의 IT 활동 등 외부 전문가(조직)를 통해 주기적 평가
CISO	· 정보보호 조직의 구성 및 운영 · 정보보호 사업 계획 수립 및 이행 · 개인정보 관리계획 중 정보보호 조치 사항의 이행 보장 · 임직원 대상 인식제고 활동 상호 협조
법무 부서	· 개인정보 보호 관련 법규 해석 책임 · 개인정보 처리방침 및 개인정보 내부 관리계획 등 법적 책임 이행에 따른 문서의 최종 검수
감사 부서	· 개인정보보호 정책 이행 현황 감사 · 주요 위반 사항 징계 절차 협력
인사 부서	· 주요 위반 사항 징계 절차 협력 · 임직원 개인정보보호 교육 및 문화 조성 활동 지원
고객 관리 부서	· 정보주체 권리 요청시 적시 이행 보장 · 정보주체 대상 안내 및 소통 책임
홍보 부서	· 주요 개인정보 보호 활동의 대·내외 홍보 · 조직의 개인정보 관련 평판에 대한 미디어 점검 · 개인정보 보호 문화 조성 지원

- (역할 · 책임 명확화) 이해관계자별 역할을 명확히 정의하여 관련된 권한과 책임을 부여하기 위해 경영진 승인 필요
  - 다양한 이해관계자와의 원활한 협업을 위해 책임 할당 차트(RACI)를 구성하여 CPO 및 이해관계자의 역할과 책임을 명확화

책임 할당 차트(RACI)

업무 절차 상의 부서/개인 간 업무에 대한 역할 및 책임 그리고 권한을 설명하는 차트

- **R**esponsible : 업무에 대해 실제 수행 책임을 지는 주체
- **A**ccountable : 업무에 대해 최종 책임을 지는 주체
- **C**onsulted : 수행과 관련하여 협업·협의가 필요한 주체
- **I**nformed : 업무 수행 결과를 보고 받는 주체

| RACI 차트 예시 |

업무 또는 활동	CEO	CPO	CISO	CIO
개인정보 보호 조직 체계 구성	I	A/R	C	C
개인정보 보호 계획 평가 및 승인	I	A/R	C	C
정보보안 체계 구축 및 운영	I	C	A/R	
개인정보 관리 체계 구축 및 운영	I	A/R	C	
수탁사 관리		A/R	C	
…	…	…	…	…
임직원 개인정보 인식 제고	I	A/R	C	
IT 도입 개발 유지보수 보안		C	C	A/R
보안 사고 대응	I	C	A/R	
개인정보 유출 사고 대응	I	A/R	C	
…	…	…	…	…

CPO 유형 결정

- (CPO 유형 결정) CPO 지정 등 개인정보 거버넌스 구성은 산업별 특성, 조직의 성격 등에 따라 다양하게 존재

- (전담 CPO) 전사적인 개인정보 보호 활동 및 위험을 신속하고 효과적으로 관리 · 감독하기 위해서는 전담 CPO 지정이 이상적

  – 단, 타 부서와의 긴밀한 의사소통이 요구되며, 안전성 확보조치 이행 · 관리를 위해 부서 내 일정 수준 이상의 정보보안 기술 역량 유지 필요

- (CPO 겸직) CISO 등 다른 직위와 겸직 가능하나 개인정보 활용에 따른 이해충돌 우려, 개인정보 보호 규제 전문성 확보 등 아래 사항 고려 필요

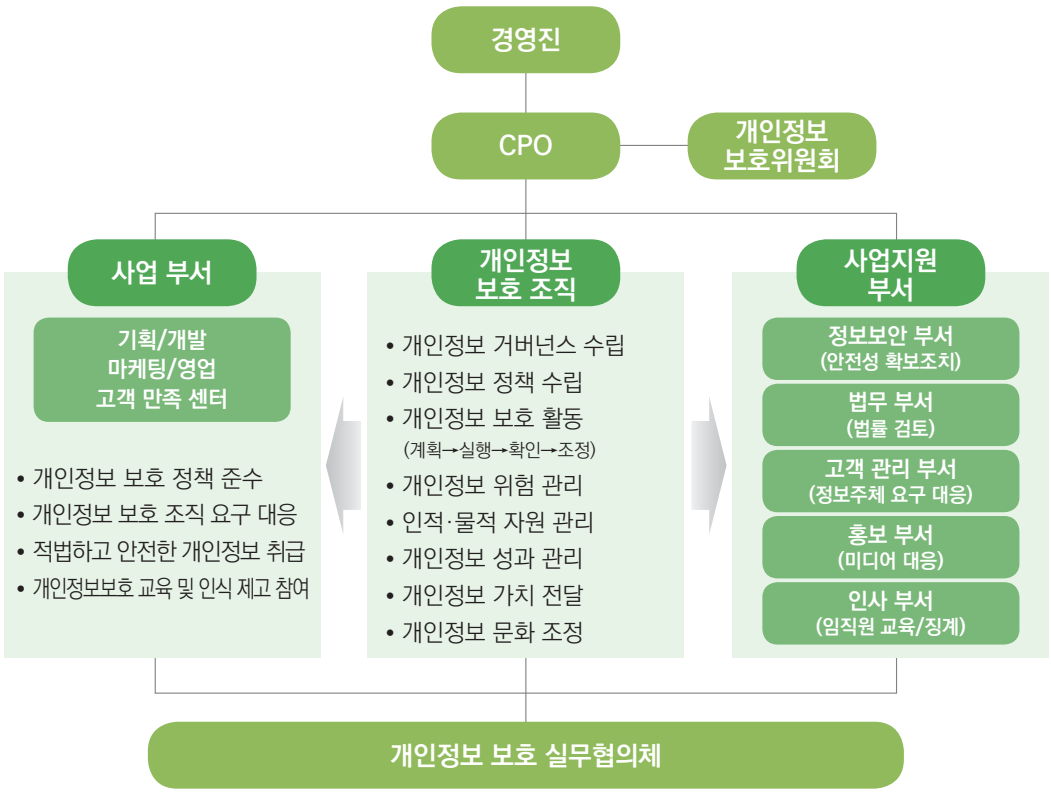
〈 CPO 겸직 시 고려 사항〉

CPO 겸직 유형	주요 고려 사항	
	특 성	유의 사항
CISO	· 개인정보보호 법 규제 대응과 기술적 보호 조치를 통합적으로 수행하여 개인정보의 안전성 확보조치, 해킹 등 사이버 공격으로 인한 개인정보 침해사고 대응의 빠른 조치가 가능	· 개인정보보호 컴플라이언스 및 기술적 지식 등 통합적 전문성이 요구되며 정보보호 업무 및 개인정보 보호 업무 간 균형을 맞추기 위한 노력 요구
법무 부서	· 개인정보 보호 법률 해석에 대한 전문성 확보 용이	· 전사적 개인정보 보호 활동에 대한 다양성 고려 필요 · 안전성 확보 조치 기준 이행을 위한 정보보호에 대한 이해, 위험 관리 체계 구축 및 운영 측면의 역량 확보에 유의
경영 지원 부서 (재무 부서 등)	· 조직내 다른 부서와 유기적 소통 및 협업 용이	· 개인정보 보호 법규, 안전성 확보 조치 기준 이행을 위한 정보보호에 대한 이해, 위험 관리 체계 구축 및 운영 측면의 역량 확보에 유의
개인정보 활용 사업 부서 겸직 (CIO, 영업, 마케팅 등)	· 개인정보 활용 현황을 보다 정확하고 효율적으로 파악 가능	· 개인정보 보호 및 활용 간 이해충돌 발생 및 개인정보보호 활동의 우선순위 저하 우려가 있음

개인정보 보호 관련 조직 구축

- 개인정보 보호 · 활용에 대한 주요 의제를 협의 및 결정하고 신속히 실행할 수 있도록 조직 체계 구축

| 개인정보 보호 조직체계 예시 |



※ 개인정보 보호 조직은 사업 부서의 개인정보 보호 활동을 점검하는 역할을 수행하고 사업 부서는 소관 업무와 관련된 개인정보 보호 활동을 수행

- (개인정보보호위원회) 개인정보 보호와 안전활용에 관한 전사적 의제를 협의하고 조직내 협업 증진, 갈등 조정 등을 위해 개인정보보호위원회 구성 및 운영 필요
  - (구성) CPO, CIO, CISO, CFO, 마케팅 및 인사 부서 등 개인정보 보호와 활용과 밀접한 관계가 있는 주요 조직의 임원으로 구성

※ 전사적 의사결정이 요구되므로 경영진이 위원장을 맡는 것이 적절하며, 임원 회의로 대체 가능

〈역할 및 주요 업무〉

역 할	주요업무
· 주요 임원들이 참여하여 전사적인 개인정보 의제를 경영적 측면에서 협의하고 결정	· 전사 주요 개인정보보호 의제에 대한 경영적 의사 결정 – 주요 관련 법규의 변화에 대한 대응 – 전사 주요 개인정보 보호 정책 도입 – 대내외 주요 개인정보 현안 대응 등 · 전사 개인정보보호 협업과 갈등 사안 처리

※ CPO는 실무협의체가 원활히 구성 · 운영되도록 유관 부서 임원 대상으로 협조 요청 필요

CPO 체크리스트

- ☐ CPO가 CEO 또는 이사회에 직접 보고할 수 있는 체계를 갖추고 있는가?
- ☐ 핵심 이해관계자 간 책임과 역할을 정의하고 조직 특성을 고려해 적절한 개인정보 보호 조직 체계를 구축하고 있는가?
- ☐ CPO, CIO, CISO, CFO, 마케팅 및 인사부서 등 개인정보 보호 및 활용 또는 경영 관련 주요 부서 임원이 개인정보 거버넌스 내 자신의 역할과 책임을 명확하게 인식하고 있는가?
- ☐ 개인정보 보호 조직이 전사적인 개인정보 업무를 수행하는 데 경영진 및 CPO의 지원은 원활하게 제공되고 있는가?
- ☐ 사내 개인정보보호위원회가 전사적인 개인정보 의제에 관해 내린 결정이 원활히 전파 및 이행되고 있는가?
- ☐ 개인정보 보호 실무협의체 통해 개인정보 보호 관련 부서의 협업이 원활하게 이뤄지고 있는가?

관련 법령

- 영 제32조(개인정보 보호책임자의 업무 및 지정요건 등)

참고자료

- 금융보안 거버넌스 가이드(금융보안원, 2019.12.)

1-2 개인정보 보호 정책[전략] 수립

• CPO는 개인정보 보호 정책과 분야별 지침을 수립하고, 사내 개인정보 처리 업무 과정에 개인정보 보호 조직의 승인, 협조 등 필요한 절차를 마련 · 운용함으로써 개인정보 보호 조직이 전사의 개인정보 관련 활동을 통제할 수 있도록 하여야 함

개인정보 보호 정책 체계

- (개인정보 보호 정책) 조직이 수행하는 개인정보 보호 활동의 근거를 포함하는 최상위 수준의 문서로서 다음 내용을 포함
  - 조직의 개인정보 보호에 관한 경영진의 의지 및 방향
  - 조직의 개인정보 보호 · 활용을 위한 역할·책임 및 대상·범위 설정
  - 개인정보 보호의 관리적·기술적·물리적 보호조치 활동

- (개인정보 보호 지침) 개인정보 보호 정책에 명시된 사항을 구체적으로 시행하기 위하여 필요한 세부 방법 등을 규정한 문서로서 보호 대상이나 수행 주체 관점에서 작성
  - (보호 대상 관점) 개인정보처리시스템 보호 지침, 개인정보 사고 대응 지침, 개인정보 파기 지침 등
  - (수행 주체 관점) 개인정보취급자 업무 지침, 개인정보 보호 교육 지침, 개인정보 보호 조직 구성 및 업무 지침 등

- (개인정보 보호 절차) 개인정보 관련 업무 수행 시 개인정보 보호 정책과 지침을 준수하기 위해 구체적으로 수행해야 하는 업무 절차
  - 각 부서에서 개인정보 관련 업무를 수행할 때 필요한 수행 절차 또는 결재 절차에 개인정보 보호 조직의 승인, 협조 등 반영

개인정보 보호 절차 예시

» 제품·서비스 기획 및 설계 시 개인정보 위험 평가 절차를 추가하고, 개인정보 보호 조직의 승인 후 다음 절차로 진행
  - 외주 용역 발주 시 개인정보 위험 평가 절차를 추가하여 개인정보의 처리 위탁 여부 평가, 필요 시 계약서 검토 수행
  - 용역 수행 시 수탁자 감독·교육 등 개인정보 처리 위탁자로서 법적 의무를 수행할 수 있도록 절차 수립

- (개인정보 보호 계획 수립) 조직의 사업 목표, 개인정보 보호 정책 등과 연계하여 연간 또는 중장기 개인정보 보호 목표를 수립하고 이를 달성하기 위한 세부 실행 계획과 전략 마련

개인정보 보호 정책[전략)] 수립 시 고려사항

- CPO는 개인정보 보호 지침과 절차의 수립·운용 시 다음 역할을 담당
  - 정보보안 관련 정책, 지침, 절차와의 정합성 검토
  - 관련 조직과의 협업을 통해 실행 가능한 지침을 만들 수 있도록 지원
  - 개별 개인정보 관련 업무 절차 수립 시 개인정보 위험 관리 가능 여부 및 해당 절차가 적절하게 운용되는지 주기적으로 점검

- 개인정보 보호 정책, 지침 등은 조직내 임직원이 이해하고 쉽게 접근할 수 있도록 전파 · 공유할 필요

CPO 체크리스트

- ☐ 회사의 개인정보 보호를 위한 정책 및 지침 등이 마련되어 있는가?
- ☐ 개인정보 보호 정책 등에 대한 이행 및 관리감독이 이루어지고 있는가?
- ☐ 전사적인 개인정보 위험을 파악하고 관리할 수 있는 절차가 있는가?
- ☐ 모든 임직원이 개인정보 보호 정책, 지침 및 절차 등에 쉽게 접근 가능한가?

2 개인정보 처리환경 분석 및 관리

2-1 개인정보 생명주기 파악

• CPO는 조직 내 서비스·시스템 별 처리하는 개인정보의 생명주기를 명확히 파악한 후 개인정보 흐름도를 최신화함으로써 개인정보 보호 내부통제의 근거를 마련하여야 함

◆ 개인정보 처리 목적 명확화

○ CPO는 개인정보처리자가 개인정보를 처리하는 목적을 우선적으로 명확하게 파악해야 하며, 처리 목적의 달성을 위해 개인정보의 처리가 필수적으로 필요한지, 필요한 경우 개인정보의 유형 및 범위 등을 정립하여야 함

- 처리 목적에 필요한 범위에서 최소한의 개인정보를 수집하여 적합하게 처리하여야 하며 그 목적 외의 용도로 활용하여서는 아니 됨
- 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성을 보장하여야 함
- 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집 목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 해야 함

◆ 처리대상 개인정보 파악

○ CPO는 개인정보처리자가 처리하는 모든 개인정보에 대해 생명주기에 따라 ①수집, ②저장·관리, ③이용·제공, ④파기 등 처리 단계별 모든 보호조치를 이행해야 함

- 정보주체의 범위*, 처리하는 개인정보의 항목·유형** 등을 파악

* 개인정보처리자가 업무 목적으로 처리하는 고객 이외에 협력사 등 외부 이해관계자 및 임직원 등 내부 이해관계자 등이 원칙적으로 포함

** 민감정보, 고유식별정보, 그 외 개인정보 등

개인정보 생명주기(Life-Cycle)

개인정보 생명주기는 개인정보를 취득하여 활용하는 단계로서 수집(Collection), 저장·관리(Storage·Management), 이용·제공(Use·Provision), 파기(Deletion) 4단계로 구분(CSUD 모델)

① 수집 : 정보주체의 개인정보를 취득하는 단계, 웹사이트 회원가입, 서면 신청서 작성, 민원 접수 등의 형태로 이루어짐

② 저장·관리 : 수집한 개인정보를 보유하는 단계, 보유한 개인정보를 안전하게 관리하며 정보주체의 개인정보 열람·정정권리 등을 보장

③ 이용·제공 : 수집·저장한 개인정보를 업무를 목적으로 이용하거나 수집한 개인정보처리자 이외의 제3자에게 개인정보를 제공하는 행위

④ 파기 : 수집 및 이용 목적이 달성된 개인정보를 파기하는 단계

※ 출처 : 개인정보 생명주기별 보안 관리모델(한국정보통신기술협회, '07.12.)

처리대상 개인정보 식별 및 체계화

- 처리하는 개인정보에 대한 명확한 파악을 위해 범위 설정 및 주요 서비스·시스템에 관한 체계화 필요
  - 조직의 핵심 서비스 및 개인정보 처리에 영향을 줄 수 있는 범위 설정
  - 개인정보 관련 주요 서비스 · 시스템 현황 파악 및 확인대상의 체계적 관리

- 서비스·시스템별 개인정보 흐름을 판별한 후 주기적으로 업데이트하여 최신화된 개인정보 흐름도로 관리 필요

  ※ 흐름도 도식화 시 서비스 또는 시스템별로 명확하게 표현 필요

  - 최신화된 개인정보 흐름도는 개인정보를 대내외적으로 통제하기 위한 기본적인 판단근거이며,
  - 서비스·시스템의 신규도입 또는 개선 과정에서 명확하고 신속한 위험관리를 가능하게 함

CPO 체크리스트

- ☐ 제공 서비스 및 시스템별 처리하는 개인정보 목록을 현행화하고있는가?
- ☐ 제공 서비스 및 시스템별 처리하는 개인정보 흐름도를 마련하고 있는가?
- ☐ 주기적인 업데이트를 통해 제공 서비스 및 시스템별 개인정보 흐름도를 최신화하고 있는가?

관련 법령

- 법 제3조(개인정보 보호 원칙)
- 법 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

2-2 개인정보처리시스템 현안파악

• CPO는 개인정보처리시스템을 파악할 수 있도록 최신성 확보, 시스템 간의 개인정보·데이터 흐름 분석, 시스템 보안(위험) 평가·개선 등의 선순환 업무체계를 갖추어야 함

개인정보처리시스템의 의미·범위

○ 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 의미(시행령 제30조제1항제2호가목)

- 개인정보처리자의 개인정보 처리 방법, 시스템 구성 및 운영환경 등에 따라 달라질 수 있으며, 작게는 한 대의 서버에서부터 크게는 수백 대의 서버 및 데이터베이스시스템(DBMS)을 운영할 수 있음

개인정보처리시스템 예시

- ✓ 데이터베이스를 구성·운영하는 시스템 그 자체
- ✓ 응용프로그램(Web 서버, WAS 등)을 데이터베이스의 개인정보를 처리할 수 있도록 구성한 경우
- ✓ 개인정보의 처리를 위해 파일처리시스템으로 구성한 경우
- ✓ 업무용 컴퓨터에 Web 서버, DBMS를 설치하고 홈페이지를 구축하여 회원가입 등을 받으면서 서비스를 제공한 경우

※ 출처 : 개인정보의 안전성 확보조치 기준 안내서(개인정보위, '24.10.)

개인정보처리시스템의 파악 및 체계적 관리

○ 개인정보처리시스템은 보호법 및 개인정보 안전성 확보조치를 직접적으로 적용해야 하는 중요 정보자산에 해당

- 개인정보처리시스템 관리 및 최신성 확보를 위해 주기적으로 조직 내 운영 중인 시스템을 파악하여 목록화
- 각 시스템 및 시스템 간 개인정보 처리 흐름을 파악하고 처리되는 개인정보의 목적과 범위를 확인
- 각 시스템에서 처리되는 개인정보 항목을 목록화하고 민감정보 및 고유식별정보 여부를 확인
- 주기적인 위험평가를 실시하고, 신규 개인정보처리시스템의 경우 개발·설계 단계에서 영향평가를 실시하는 것이 바람직
- 개인정보처리시스템 목록, 개인정보 흐름도 등을 문서화하고 정기적 업데이트를 통해 최신성 유지

CPO 체크리스트

□ 개인정보처리시스템에 대해 명확히 파악하고, 정기적으로 업데이트 하고 있는가?

□ 개인정보처리시스템에 대한 접근권한 부여 등 접근통제, 접속기록 관리 등 안전성 확보조치 준수 여부에 대해 주기적으로 점검 및 개선하고 있는가?

관련 법령

- 법 제29조(안전조치의무)
- 법 제31조(개인정보 보호책임자의 지정 등)
- 영 제30조(개인정보의 안전성 확보조치)

참고자료

- 개인정보의 안전성 확보조치 기준 안내서(개인정보위, 2024.10)

2-3 개인정보파일 관리 및 현행화

• 개인정보 파일은 정보주체의 개인정보를 처리하는 단위로서 CPO는 조직 내 처리되는 개인정보 파일에 대한 명확한 파악·분류 및 이에 대한 안전성 확보조치가 제대로 구현되어 있는지에 대해 주기적으로 점검하고 개선할 필요가 있음

◆ 개인정보파일의 의미 · 범위

○ 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 의미(법 제2조 제4호)

- DB 등 전자적 형태뿐만 아니라 수기(手記)문서 자료도 포함
- 개인의 이름, 고유식별정보, ID 등을 색인(index)이나 검색 값으로 하여 쉽게 검색할 수 있도록 체계적으로 배열·구성한 집합물이면 개인정보파일에 해당

※ 블랙박스로 촬영된 영상정보는 촬영일시 등에 따라 체계적으로 배열하여 저장되므로 개인정보파일에 해당 (개인정보보호위원회 결정 제2017-13-100호)

개인정보파일의 범위 관련 동향

» EU의 GDPR, 영국·일본 개인정보 보호법에서도 모든 개인정보가 아니라 특정한 파일체계로 구성하고 있거나, 그런 의도로 처리된 개인정보에 한해 법령의 적용을 받도록 규정

- 개인정보가 기재되어 있는 단순한 집합물에 불과하고 체계적으로 배열·검색할 수 있도록 구성되어 있지 않은 경우, 개인정보파일에 해당되지 않는다고 볼 수 있음
- 다만, 최근 생성형 AI 기술의 발전으로 '체계적 배열·검색'의 범위가 탄력적으로 확대되어, 개인정보파일 범위도 확대되어 평가될 소지가 있음

◆ 개인정보파일 현행화

○ 개인정보파일은 정보주체의 개인정보를 처리하는 단위로서

- CPO는 개인정보파일의 보호 및 관리·감독 책임 필요(법 제31조제3항제6호)
- 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 함(법 제33조제11항)

○ 또한, CPO는 조직 내 모든 개인정보파일을 명확히 파악하고 분류하는 역할을 주기적으로 현행화하여야 함

CPO 체크리스트

□ 조직 내 처리되는 개인정보 파일의 현황에 대해 주기적으로 확인하고 있는가?

□ 개인정보 파일에 대한 접근권한 부여 현황, 각 파일에 대한 보유기간 설정, 만료 후 파기절차 구현 여부 등에 대해 주기적으로 점검 및 개선하고 있는가?

관련 법령

- 법 제29조(안전조치의무)
- 법 제31조(개인정보 보호책임자의 지정 등)
- 법 제33조(개인정보 영향평가)
- 영 제30조(개인정보의 안전성 확보조치)

참고자료

- 개인정보의 안전성 확보조치 기준 안내서(개인정보위, 2024.10.)

3 개인정보 보호 활동

3-1 개인정보 수집 · 이용 및 제공 적법성 관리

• CPO는 개인정보를 수집하거나 제3자에게 제공하기 이전에 법적 요구사항을 사전에 분석하여 적법하게 수집하거나 제3자에게 제공되도록 관리 · 감독할 필요가 있음

◆ 개인정보 수집·이용 및 제3자 제공 시 적법성 검토

○ CPO는 개인정보 수집 · 이용* 또는 제3자 제공 이전에 주요 사항**에 관해 사전 확인하여 적법성 여부 검토 필요

* (수집 · 이용) 수집 · 이용 목적 및 항목, 보유 · 이용기간, 수집 · 이용 근거 등

** (제3자 제공) 제공받는 자, 제공 목적, 제공 항목, 보유 · 이용기간, 제공 근거 등

– (적법성 검토) 개인정보 수집·이용 또는 제3자 제공에 관하여 적법하게 처리하는지 여부 확인

① (적법한 처리 근거 확인) 해당하는 법 조항을 검토하고 적법하게 처리하기 위한 근거 확인

가) 개인정보 수집·이용에 관하여 법 제15조제1항제1호부터 제7호 중 어디에 해당하는지 검토

나) 개인정보 제3자 제공에 관하여 법 제17조제1항제1호부터 제2호 중 어디에 해당하는지 검토

다) 개인정보 목적외 이용·제공에 관하여 법 제18조제2항제1호부터 제10호* 중 어디에 해당하는지 검토

* 제5호부터 제9호까지는 공공기관만 해당

라) 당초 수집 목적과 합리적 범위 내 추가 이용 또는 제공에 해당하는지 검토

② (민감정보·고유식별정보 처리) 수집·이용 또는 제3자 제공 항목에 민감정보 또는 고유식별정보 처리 시 적법하게 처리하기 위한 근거 확인

가) 민감정보 또는 고유식별정보 처리에 관하여 법령에 구체적으로 허용하고 있는지 검토

나) 법령에 구체적으로 허용하고 있지 않는 경우라면 별도 동의를 받도록 하고 있는지 확인

다) 특히, 주민등록번호 처리에 관하여 법 제24조의2제1항에 따라 적법하게 처리되는지 확인

③ (만 14세 미만 아동 정보 처리) 동의를 받아야 하는 경우로써 만 14세 미만 아동의 개인정보 처리 시 법정대리인 동의 여부 확인

- (동의받는 방법 검토) 개인정보 수집·이용 또는 제3자 제공에 관하여 동의를 받을 경우 동의 안내 및 구분 동의를 준수하고 있는지 확인

  ① (동의 안내 확인) 개인정보 수집·이용 또는 제3자 제공 동의 안내 사항을 모두 준수하고 있는지 확인

  ※ 수집·이용 동의 안내(수집·이용 목적, 수집·이용 항목, 보유 및 이용기간, 동의거부 시 불이익 내용), 제3자 제공 동의 안내(제공받는 자, 제공 목적, 제공 항목, 보유 및 이용기간, 동의거부 시 불이익 사항) 내용의 적정성도 확인

  ② (구분 동의 확인) 각각 동의사항을 구분하여 동의를 받아야 할 사항 검토

  ③ (중요내용 표시) 동의를 서면(전자문서 포함)으로 받는 경우, 동의한 내용을 명확하게 표시하였는지 검토

  ④ (서비스 제공 거부 금지 준수) 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나, 목적 외 이용 · 제공 동의 및 재화나 서비스를 홍보, 판매권유를 위한 동의를 하지 아니한다는 이유로 서비스 제공을 거부하지 않아야 하므로 이를 준수하고 있는지 확인

- (동의받지 않는 경우 공개사항 검토) 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적근거를 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침 등에 공개여부 검토

개인정보 수집·이용 및 제3자 제공 동의서 관리

- (관리 절차) CPO는 각 부서에서 작성한 동의서를 사용하기 전에 적정 여부를 확인하고 관리 · 감독할 수 있도록 내부 절차를 마련
  - 체계적인 동의서 관리를 위해 아래와 같은 절차 고려

절 차	주요내용	업무담당
1. 동의서 작성 매뉴얼 마련	· 각 부서에서 동의서 작성 시 매뉴얼을 참고하여 작성할 수 있도록 함 · 매뉴얼 내에는 동의서 작성에 대한 전반적인 절차를 반영 · 작성된 매뉴얼은 인트라넷 등에 배포	개인정보 보호 조직 (개인정보 보호 담당자)
⬇		
2. 동의서 작성	· 각 부서는 매뉴얼을 기반으로 개인정보 수집·이용 또는 제3자 제공 동의서 작성	업무부서
⬇		
3. 동의서 검토	· 동의서가 법 제15조, 제16조, 제17조, 제18조, 제19조, 제22조, 제23조, 제24조 등 법적 요구사항을 준수하는지 검토	법률 담당자, 개인정보 보호 담당자
⬇		
4. 동의서 승인	· 동의서 검토가 완료되면 CPO에게 보고 및 승인	CPO

개인정보 수집·이용 및 제3자 제공 적법성 관리·감독

- (관리·감독) 개인정보 수집·이용 및 제공 현황 시 목적외 이용, 제공 등의 여부를 주기적(연 1회 이상)으로 관리·감독
  - 수집목적 이외로 이용하거나 제3자에게 제공하는지 여부
  - 운영하는 동의서 서식의 변경에 따른 법적사항 준수 여부
  - 개인정보 수집·이용 및 제공 동의서 원본은 시건장치 등을 통해 안전하게 관리되고 있는지 여부

CPO 체크리스트

□ 개인정보 수집·이용 또는 제3자 제공 전에 적법성을 검토하였는가?

□ 개인정보 수집·이용 또는 제3자 제공 시 동의서 작성에 대한 절차를 마련하였는가?

□ 개인정보 수집·이용 또는 제3자 제공 시 적법하게 처리되고 있고 동의서 원본을 안전하게 관리를 하고 있는지에 대해 주기적으로 관리·감독하고 있는가?

관련 법령

- 법 제15조(개인정보의 수집·이용)
- 법 제16조(개인정보의 수집 제한)
- 법 제17조(개인정보의 제공)
- 법 제18조(개인정보의 목적 외 이용·제공 제한)
- 법 제19조(개인정보를 제공받은 자의 이용·제공 제한)
- 법 제22조(동의를 받는 방법)
- 법 제22조의2(아동의 개인정보 보호)
- 법 제23조(민감정보의 처리 제한)
- 법 제24조(고유식별정보의 처리 제한)
- 법 제24조의2(주민등록번호 처리의 제한)
- 영 제17조(동의를 받는 방법)
- 영 제18조(민감정보의 범위)
- 영 제19조(고유식별정보의 범위)

참고자료

- 알기쉬운 개인정보 처리 동의 안내서(개인정보위, 2022.3)

3-2 개인정보 처리방침 관리

• CPO는 개인정보 처리방침을 수립하여 개인정보 처리의 투명성을 높이고, 정보주체가 알기 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 공개해야 하며 지속적으로 현행화 등 변경관리를 하여야 함

개인정보 처리방침 수립

○ 처리방침 수립을 위해서 아래와 같은 사항을 사전에 파악하여 현행화하는 것이 중요하며, 개인정보 관련 내부 정책 등을 통해 세부사항을 확인하여 처리방침 수립의 기초 자료로 활용

- 부서별 개인정보 처리 현황*

  * 처리목적, 처리항목, 보유 및 이용기간, 공공기관의 경우 개인정보파일 포함

  ※ 동의 없이 개인정보 수집·이용하는 경우는 수집근거 포함

- 개인정보 제3자 제공 현황*

  * 제공받는 자, 제공 목적, 제공하는 개인정보 항목, 보유 및 이용기간

  ※ 동의 없이 제3자 제공하는 경우는 제공근거 포함

- 개인정보 처리 업무 수탁자(재수탁자 포함) 및 위탁업무 내용
- 개인정보 파기 절차 및 방법
- 부서별 가명정보의 처리 현황*

  * 내부적 활용 또는 제3자 제공 유무

- 정보주체 권리보장 내용 및 현황*

  * 열람, 정정·삭제, 처리정지, 자동화된 결정 대응권 등

- 클라우드 서비스 등을 통한 국외 이전 현황
- 개인정보를 안전하게 관리하기 위한 관리적, 물리적, 기술적 보호조치 현황

○ (처리방침 작성) 선행 작업을 통해 파악된 내용을 기반으로 개인정보 처리방침을 작성

- (법령 적합성) 법 제30조제1항 각호의 사항을 확인하여 누락 없이 작성, 동의 없이 처리하는 경우와 동의를 받고 처리하는 경우를 구분하여 작성

  ※ 각호의 사항에 해당되지 않은 경우는 작성하지 않아도 무방

- (가독성 제고) 정보주체가 개인정보 처리방침의 내용을 알기 쉽게 작성
- (투명성 제고) 개인정보 처리현황을 정확하게 반영하도록 개인정보 처리목적, 개인정보의 처리 및 보유기간, 처리하는 개인정보 항목은 연계성을 고려하여 일관성 있게 작성

개인정보 처리방침 공개

- (관리 절차) 개인정보 처리방침은 CPO 관리·감독 하에 개인정보 보호 담당 검토 후 외부에 공개
- (접근성 제고) 웹·모바일 앱 등 서비스 환경을 고려하여, 인터넷 홈페이지 등에 정보주체가 쉽게 확인할 수 있도록 공개

  ※ 인터넷 홈페이지가 없거나 게재하기 어려운 경우는 사업장 등 확인이 용이한 장소에 게시

개인정보 처리방침 변경 등 이력관리

- (현행화) 개인정보 처리 내역 등의 변경 사항을 주기적 점검을 통해 현행화 유지 필요
  - 개인정보 처리목적, 처리항목, 처리 및 보유기간 변경 관리
  - 개인정보 처리 업무 위탁, 제3자 제공 현황 변경 관리
  - 이 외에 조직변경에 따른 담당자 변경 등 현황 관리
- (이력관리) 처리방침의 내용 변경이 필요한 경우 지체 없이 반영하고 이에 따른 이력관리 수행 (변경 및 시행시기, 변경내용 등) 수행

CPO 체크리스트

- ☐ 개인정보 처리방침 수립을 위한 개인정보 처리 현황 분석 등 선행업무를 수행하였는가?
- ☐ 개인정보 처리방침을 수립하여 공개하고 있는가?
- ☐ 개인정보 처리방침에 대한 관리·감독을 통해 현행화하고 있는가?
- ☐ 개인정보 처리방침에 대한 변경관리를 하고 있는가?

관련 법령

- 법 제30조(개인정보 처리방침의 수립 및 공개)
- 법 제30조의2(개인정보 처리방침의 평가 및 개선권고)
- 영 제31조(개인정보 처리방침의 내용 및 공개방법 등)

참고자료

- 개인정보 처리방침 작성지침(개인정보위, 2024.4.)

3-3 개인정보취급자 관리

• CPO는 개인정보취급자 현황을 파악하고 개인정보 오·남용 및 유출 등의 방지를 위해 개인정보취급자 대상으로 정기적인 인식제고 교육 등 관리·감독을 하여야 함

◆ 개인정보취급자 현황 파악 및 현행화

○ (현황 파악) 개인정보취급자의 체계적 관리를 위해 아래 사항을 주기적으로 검토

- 직원(외부 용역, 수탁자 직원 포함) 중 개인정보를 처리하는 자*를 개인정보취급자로 구분하고 현황 파악

  * 임직원, 파견근로자, 시간제근로자

- 개인정보취급자를 최소한으로 제한하고 있는지 확인
- 개인정보 처리 업무의 중요도에 따라 개인정보취급자 유형 구분 · 관리

  ※ 개인정보취급자 유형별 권한 등으로 차등화하여 관리 필요

○ (현행화) 개인정보취급자의 업무, 유형 등의 현황을 주기적으로 현행화하여 문서 등으로 체계적 관리

◆ 개인정보취급자 관리·감독

○ (서약서) 개인정보취급자가 개인정보 처리 업무를 수행하기 전에 보안서약서를 제출하도록 함

- 개인정보취급자가 개인정보 보호에 대한 경각심을 갖도록 보안서약서는 매년 갱신하여 받도록 권장

○ (취급자 교육) 매년 개인정보 보호교육 계획을 수립하여 개인정보취급자별 차등화된 교육을 시행하도록 함

- 개인정보취급자 유형에 따른 차등화된 교육 계획 수립
- CPO는 교육계획에 따라 교육을 시행하도록 하고 개인정보취급자 모두 정기적으로 교육을 받도록 해야 함
- 교육 효과성, 개선사항 등을 분석하여 차년도 교육 계획에 반영

교육대상(예시)

개인정보취급자 유형별 차별화된 개인정보 보호교육 계획에 반영되어야 할 교육대상(예시)

- CPO(전문성을 갖추기 위해 교육계획에 반영)
- 개인정보 보호 조직 내 직원 및 개인정보 보호 담당자
- 부서별 개인정보 보호책임자 및 관리자
- 부서별 개인정보 보호 담당자
- 개인정보처리시스템 개발자 및 운영자
- 개인정보 처리 부서 직원(고객응대 직원, 사무업무 수행 직원 구분하여 차별화 고려)
- 개인정보 처리 업무를 위탁받은 수탁자 직원
- 그 외 개인정보처리자 업무특성에 따른 개인정보취급자 유형 등

CPO 체크리스트

- ☐ 개인정보취급자 현황을 유형별로 파악하고 관리하고 있는가?
- ☐ 보안서약서를 제출받고 관리하고 있는가?
- ☐ 매년 개인정보취급자별로 차등화된 교육 계획을 수립하여 정기적으로 시행하고, 그 결과를 평가하고 있는가?
- ☐ 개인정보 보호 캠페인 등 인식제고 활동을 하고 있는가?

관련 법령

- 법 제28조(개인정보취급자에 대한 감독)
- 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

3-4 개인정보 처리 업무 위탁 관리

• CPO는 개인정보 처리 업무 위탁 시, 수탁자가 개인정보를 안전하게 처리할 수 있도록 관리·감독할 수 있는 절차를 마련하여 계약 종료까지 체계적으로 관리해야함

단계별 관리 방안

- (업체 선정 단계) 개인정보 보호 역량을 갖춘 업체를 선정할 수 있도록 내부 기준 등 체계 마련
  - (점검지표) 사업부서에서 업체 선정 시 개인정보 보호 역량*을 평가할 수 있도록 '개인정보 처리업무 위탁 점검지표' 등을 마련·제공
    * 위탁 업무 중에 수탁자가 운영하는 시스템이 포함될 경우 개인정보 안전성 확보조치 기준 준수 등 보호조치 여부 검토
  - (점검지표 검토) 개인정보 담당 부서는 사업부서가 작성한 점검지표를 검토하여 적정한 업체가 선정되었는지 확인 후 CPO에게 보고

- (계약 단계) 위탁할 업무범위를 명확히 하고 최소한의 개인정보가 처리될 수 있도록 법 제26조 제1항의 내용을 포함하여 문서화
  - (위탁 문서) 개인정보 처리업무 위탁 계약 시 반영할 수 있도록 표준화된 문서 마련 필요

업무 위탁 계약시 고려사항

CPO는 아래와 같은 표준화된 문서를 작성하여 업무 위탁 계약 시 반영하도록 계약부서에 제공

- 법 제26조제1항의 내용을 포함한 표준화된 문서(예 : 개인정보 처리 업무 위탁 계약서)
  ※ 개인정보위, 표준 개인정보 처리 위탁 계약서 참조
- 수탁자가 제3자에게 업무를 다시 위탁 시 동의 서식 문서(예 : 업무 재위탁 동의 확인서)
- 재위탁 업체명, 재위탁 업무 범위 및 내용, 계약기간 등 내용 작성
- 수탁자 대표자 직인(필)
- 수탁자 대표자 및 수행 인력에 대한 보안 서약서

- (위탁 절차) 업무 위탁 계약 절차 내 개인정보 담당 부서의 결재를 추가 하는 등 현황 파악을 위한 절차 마련
- (위탁 공개) 계약된 수탁자명, 업무내용(재위탁시, 재위탁 사항 포함)에 대해서는 개인정보 처리방침에 공개
- (위탁 관련 교육) 사업부서가 계약 체결 시 ① 위탁할 업무 범위를 명확하고 구체적으로 정의, ② 수탁자에게 개인정보 제공은 최소화, ③ 개인정보 관련 책임 소재 명확화 등을 고려할 수 있도록 정기적으로 교육 실시

◎ (수행 단계) 수탁자의 개인정보 관리 체계, 기술적·물리적 보호 조치의 적절성 여부 등 관리·감독 수행

- (교육시행) 위탁 업무 수행 전에 위탁 업무 유형을 고려하여 맞춤형 개인정보 보호 교육 콘텐츠를 마련하여 수탁자 직원을 대상으로 교육 시행

  ※ 위탁 업무 수행 기간 내 정기적(예 : 연 1회 이상)으로 실시

수탁자 개인정보 보호 교육 방안

- 업무 위탁 유형에 따라 교육 내용의 차별화
- 수탁자 직원이 실질적으로 개인정보 보호 역량을 높일 수 있도록 교육 내용 반영
- 수탁자 대상으로 교육 수행
  - 위탁자가 직접 교육 수행
  - 개인정보 보호 교육 전문가, 전문 교육 기관 등을 통해 수탁자 교육 수행
  - 수탁자 자체적으로 교육 수행(이 경우, 교육 증빙 자료를 위탁자에게 제출)

- (실태점검) 수탁자가 계약 및 법 제29조의 안전조치 등을 준수하여 개인정보를 안전하게 처리하고 있는지 감독 수행을 위한 점검 지표를 작성하여 정기적(연 1회 이상)으로 개인정보 관리 실태 점검 수행

  ※ 업무 위탁 유형, 업무 위탁 성격, 개인정보의 보유량, 개인정보 업무 역량 등을 고려하여 점검 지표를 마련하여 수탁자의 개인정보 관리 실태를 점검하는 것이 바람직

◎ (종료 단계) 수탁자 대상 제공했던 개인정보 파기 또는 반환 확인 및 증빙자료 확보

- 계약이 종료된 위탁 업무와 관련된 개인정보가 파기 또는 반환되었는지 확인하고 이에 대한 증빙자료를 확인

  ※ 수탁자의 지위에 있는 CPO 경우, 법 제26조 제 5항, 제6항, 제8항에 따른 업무 수행 및 위탁사 요청에 따른 추가적 조치 이행 필요

CPO 체크리스트

- ☐ 업체 선정 시 개인정보 보호 역량을 갖춘 업체 선정을 위한 기준을 마련하고 있는가?
- ☐ 개인정보 처리업무 위탁 계약 시 표준화된 문서를 마련하고 있는가?
- ☐ 수탁자 개인정보 처리 업무에 대한 관리·감독을 주기적으로 수행하고 있는가?
- ☐ 계약 종료 시 수탁자의 개인정보 삭제 및 회수에 대한 관리·감독을 수행하고 있는가?

관련 법령

- 법 제26조(업무위탁에 따른 개인정보의 처리 제한)

참고자료

- 개인정보 처리 위수탁 안내서(개인정보위, 2020.12.)

3-5 개인정보처리시스템 보호조치 관리

• CPO는 개인정보처리시스템에서의 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 않도록 내부 관리계획 등 개인정보 정책에 따라 보호조치를 수행하고 있는지에 대한 관리 · 감독을 수행하여야 함

◆ 개인정보 유출 보호조치

○ (접근통제) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 안전조치 시행

- 개인정보처리시스템에 대한 접속 권한을 IP 주소, 포트, MAC 주소 등으로 제한하여 인가받지 않는 접근을 제한하도록 침입차단 시스템 구축(예 : 방화벽 등)
- 개인정보처리시스템에 접속한 IP 주소, 포트, MAC 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지·차단할 수 있는 시스템 구축(예 : IPS, 웹 방화벽 등)

○ (운영·관리) 침입차단시스템, 개인정보 유출 탐지·차단 시스템 및 접근권한 등에 대한 정책 설정 및 운영·관리

- 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 구축된 시스템에 대한 정책 설정의 현행화
- 개인정보처리시스템 이상 행위 대응, 로그 훼손 방지 등 관련 시스템의 안전성 확보를 위한 운영·관리 수행
- 개인정보처리시스템에 부여된 접근권한에 대한 주기적 점검 및 관리

○ (취약점 점검) 취약점 등에 대한 기술적 보호조치를 강화하고 주기적 점검을 통해 개선조치 등 노력 필요

- 개인정보 보호 계획 수립 시 개인정보를 안전하게 보호하기 위한 기술적 보호조치 반영
- 개인정보처리시스템에 대한 주기적(연 1회 이상) 취약점 점검을 실시하고 적절한 개선조치 수행

※ 언론 등을 통해 신규 취약점이 확인된 경우, CPO는 지체없이 취약점 점검을 수행

개인정보 오·남용 방지 보호조치

- (접속기록 관리) 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 내역을 알 수 있도록 접속기록 관리
  - (관리항목) 접속기록은 개인정보의 안전성 확보조치 기준 제2조에 정의된 5가지 항목*이 기록되도록 관리

    * 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행 업무 등
  - (보관) 접속기록은 최소 1년 또는 2년 이상 보관하도록 하고 위·변조 및 도난, 분실되지 않도록 안전하게 보관 및 관리

2년 이상 보관·관리 필요 대상

- 개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)에 따라 다음에 해당하는 경우 접속기록을 2년 이상 보관 · 관리할 필요
  - 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
  - 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
  - 개인정보처리자로서 「전기통신사업법」 제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

- (접속기록 점검) 개인정보처리시스템의 접속기록을 월 1회 이상 정기적으로 점검하여 비정상 행위를 탐지하고 적절한 대응 조치 수행

CPO 체크리스트

- □ 정보통신망을 통한 불법적인 접근 및 침해사고 등 안전성 확보를 위한 보호조치를 하고 있는가?
- □ 개인정보처리시스템의 유출 등 침해사고 예방을 위해 취약점 및 법 위반 요소에 대한 주기적 점검을 통해 기술적 보호조치 노력을 하고 있는가?
- □ 개인정보처리시스템에 대한 접속기록 관리 및 주기적 점검을 수행하고 있는가?

관련 법령

- 법 제29조(안전조치의무)
- 영 제30조(개인정보의 안전성 확보조치)
- 개인정보의 안전성 확보조치 기준

3-6 개인정보 파기 관리

• CPO는 처리 중인 개인정보에 대하여 목적을 달성하거나 보유기간이 경과되면 지체없이 파기할 수 있는 절차를 마련하고 파기가 제대로 수행되는지에 대한 관리·감독을 수행하여야 함

◆ 파기 대상 확인 및 파기 절차 마련

○ (대상 확인) 처리목적이 달성되거나 보유기간이 경과되어 파기되어야할 개인정보 파악

파기 대상 개인정보

- ✓ 수집·이용 동의를 받을 때 안내되었던 보유기간이 경과된 개인정보
- ✓ 법령 등에서 안내된 보유기간이 경과된 개인정보
- ✓ 회원탈퇴, 제명, 계약관계 종료, 동의철회 등에 따른 개인정보 처리의 법적 근거가 소멸된 개인정보
- ✓ 해당 서비스 또는 사업 종료로 더 이상 처리되지 않는 개인정보
- ✓ 이벤트 서비스 등 일시적 서비스로 수집·이용된 개인정보
- ✓ (공공기관에 해당) 개인정보파일별 보유기간이 경과된 개인정보

○ (보유형태 확인) 파기 대상 개인정보 보유형태(문서, 전자파일, DB 등) 및 현황을 파악하여 누락 없이 파기 필요

개인정보 보유 형태

- ✓ (문서) 문서고 등 지정된 장소 외에 부서별 별도 장소에 보관 여부 확인
- ✓ (전자파일) 파일서버 등 지정된 장소 외에 부서별 별도 서버 및 업무용 컴퓨터에 보관 여부 확인
- ✓ (DB) 개인정보처리시스템 별 개인정보 파기 대상 DB 현황 확인

○ (파기 방법 · 절차) 파기 대상 및 유형별 파기가 체계적으로 수행될 수 있도록 방법 및 절차 마련

개인정보 파기 관리·감독

○ 개인정보 보유 형태에 따라 적절한 방법으로 지체없이* 파기하고, 복구 또는 재생되지 않는지 확인

* 해당 개인정보가 불필요하게 된 때로부터 5일 이내(표준 개인정보 보호지침 제10조)

개인정보 보유 형태별 파기 관리·감독 방법

- 파쇄, 소각 등을 통해 파기가 제대로 수행되었는지 실사를 통해 확인하고 파기대장 등을 기록 · 관리문서가 제대로 파기되고 있는지 확인
- 업무용 컴퓨터, 파일서버 등에 보유한 전자파일이 복구 또는 재생되지 않도록 파기가 제대로 수행되었는지 실사를 통해 확인
  - 개인정보처리시스템 간 연계 수행을 위한 연계시스템 내 임시 전자파일이 지체 없이 파기 수행되고 있는지 확인

    ※ 전자파일 파기 현황을 효율적으로 관리·감독을 수행할 수 있도록 파기 솔루션 등을 활용하는 방안 고려
- 개인정보처리시스템 DB 내 개인정보가 복구 또는 재생되지 않도록 파기가 제대로 수행되었는지 실사를 통해 확인
  - 개인정보처리시스템 내 자동 파기되도록 구현된 경우 정상적으로 수행되고 있는지, 개인정보처리시스템 DB내 파기 대상 정보가 여러 테이블에 저장된 경우 모두 제대로 파기되고 있는지 확인
- 하드디스크 등에 저장된 개인정보 파기 시 복구 또는 재생되지 않는지 확인
  - 정보자산 폐기 시 하드디스크 재사용을 할 경우 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행이 제대로 수행되었는지 확인

    ※ 정보자산 폐기 시 디가우저 등 전용 장비를 활용하는 방안 고려(문서) 문서고 등 지정된 장소 외에 부서별 별도 장소에 보관 여부 확인

CPO 체크리스트

- □ 개인정보 파기를 위한 업무 절차를 마련하고 있는가?
- □ 개인정보 파기 대상 현황 파악 및 현행화를 하고 있는가?
- □ 개인정보 파기에 대한 관리·감독을 수행하고 있는가?

관련 법령

- 법 제21조(개인정보의 파기)
- 표준 개인정보 보호지침 제10조(개인정보의 파기방법 및 절차)

3-7 정보주체 권리보장

• CPO는 정보주체의 권리 보장을 위해 조직 내 표준화된 대응 절차를 수립하여 적시에 효율적으로 처리될 수 있도록 조치하고 처리 현황을 주기적으로 점검할 필요가 있음

◆ 권리보장 절차 수립

○ (정보주체 권리 확인) 법에 규정된 정보주체 권리 중 조직의 개인정보처리 활동과 관련된 정보주체 권리를 확인

정보주체 권리보장 확인사항

✓ (개인정보처리자 공통 적용) 법 제35조 개인정보의 열람, 제36조 개인정보의 정정·삭제, 제37조 개인정보의 처리 정지 등

✓ (사업 관련성 분석 시) 법 제38조 자동화 결정, 제39조 개인정보 전송 요구권 등

○ (정보주체 권리보장 창구) 개인정보 처리방침 통해 안내된 창구 외에도 대표 전화번호, 이메일 등 정보주체가 쉽게 접근 가능한 창구 확인

○ (표준 절차 마련) 유관 부서와 협의하여 정보주체 권리 유형별로 아래 사항을 고려하여 표준화된 처리 절차를 마련

- 정보주체 접수 후 10일 이내 처리 완료
- 권리 행사자가 해당 개인정보의 정보주체 또는 정당한 대리인인지 확인
- 개인정보 수집 방법보다 용이한 절차 마련
- 권리행사 처리 제한, 연기 또는 거절에 대한 절차

○ (매뉴얼화) 고객센터 등 정보주체 접점 부서를 대상으로 표준화된 처리 절차를 기반으로 대응 매뉴얼을 마련하도록 요청

- 개인정보 보호 조직이 대응 매뉴얼을 검수할 수 있도록 내부 절차를 마련하고, 매뉴얼에 따라 대응할 수 있도록 관련 부서 대상 교육 실시

정기적 점검

- (정기 점검) 고객 관리 부서 등 유관 부서를 대상으로 정보주체 권리행사 요구에 대한 적시 처리 여부를 주기적으로 점검하고 현황을 공유

  ※ 개인정보 관련 민원의 민감성을 고려하여 고객센터 내 '개인정보 권리대응 전담 부서' 설치 또한 고려 가능

  – (기타 접점 확인) 개인정보 처리방침 내 기재된 공식 접수 창구 외에도 회사 대표 이메일, 채팅 상담, 전화 등 정보주체가 접근 가능한 창구의 정상 작동 여부 및 대응 현황을 주기적으로 확인

CPO 체크리스트

- ☐ 조직의 개인정보처리 활동과 관련된 정보주체 권리를 식별하였는가?
- ☐ 정보주체의 권리 행사가 가능한 접점을 식별하였는가?
- ☐ 정보주체 권리별 처리절차를 표준화하였는가?
- ☐ 고객센터 등 유관 부서 대상 표준화된 처리절차를 전파하고 교육하였는가?
- ☐ 정보주체 권리 행사 및 처리 현황을 주기적으로 모니터링하고 있는가?

관련 법령

- 법 제35조(개인정보의 열람)
- 법 제35조의2(개인정보의 전송 요구)
- 법 제36조(개인정보의 정정·삭제)
- 법 제37조(개인정보의 처리정지 등)
- 법 제37조의2(자동화된 결정에 대한 정보주체의 권리 등)
- 법 제38조(권리행사의 방법 및 절차)

3-ㅂ 개인정보 처리 실태 및 관행의 정기적 조사

• CPO는 전사적 개인정보 보호 활동 이행현황을 대해 주기적으로 파악하고 보호활동의 적절성을 확인하여 주요 사항에 대해서는 경영진을 대상으로 보고하고 취약점에 대한 개선조치 및 재발 방지를 유도하는 등 조직의 개인정보 관련 위험을 관리할 필요가 있음

◆ 점검 계획 수립

○ (대상 및 범위) 전사적인 관점에서 개인정보 처리와 관련된 업무, 조직, 시스템, 수탁자 등 전 영역을 점검 범위에 포함

- 전 영역 점검을 원칙으로 하되, 처리하는 개인정보의 유형 및 민감도, 보유량 등 위험에 기반하여 점검 주기 및 항목, 방법 등 차등화

○ (점검 항목) 관련 법규의 제·개정 여부를 지속적으로 파악하여 개인정보 처리에 미치는 영향 분석 및 점검항목의 최신성 유지

- 개인정보 생애주기에 따른 법적 요구사항 및 내부 정책 준수 여부
- 접근 권한 관리, 접속기록 보관 및 점검 등 내부 관리계획 이행 실태
- 개인정보 보호 기술 및 환경 등에 따른 위험 대응 수준 등

○ (점검 주기) 최소 연 1회 이상 정기적으로 점검을 수행하도록 계획을 수립하고, 개인정보 보호 관련 법규의 제·개정, 새로운 취약점 및 위협, 유사 침해사고 등을 고려하여 추가 점검 수행

개인정보 안전성 확보조치 기준

제4조(내부 관리계획의 수립 · 시행 및 점검) ④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검 · 관리 하여야 한다.

○ (점검 조직 및 방법) 독립성 및 전문성을 고려하여 점검 조직을 구성하고 관련 부서별 역할 및 책임을 명확히 정의

- 점검 대상의 특성, 위험 수준 등을 고려하여 현장점검, 원격점검, 자가점검 등 적절한 방법 선정

점검 계획 공유 및 점검 실시

- (계획 공유) 점검 대상 부서 등 유관 부서를 대상으로 점검 계획 공유
  - CPO는 유관 부서 부서장을 대상으로 계획안의 공유 및 점검 협조 요청, 사내 개인정보보호위원회 등에 점검 계획 사전공유 등을 통해 원활한 점검이 이루어지도록 의사소통 수행
    ※ 필요시 설명회 등을 통해 유관 부서의 개인정보 보호 역량 강화의 기회로 활용
- (점검 실시) 계획에 따라 점검을 수행하고 결과를 분석 및 정리
  - 필요시 유관 부서에 추가 자료를 요청하여 점검 결과를 보완하고 개선 방안을 논의 후 점검 결과 보고서 작성

점검 결과의 보고 및 개선조치

- (경영진 보고) 경영진이 참석하는 임원 회의를 통해 주요 점검 결과 및 개선 계획을 보고하고 관련 부서에 개선 요청을 하는 것이 효과적
  - 특히, 중대한 영향을 초래할 수 있는 사안 등은 CPO가 사업주(대표)·이사회 등에게 보고 후, 의사결정 절차를 통하여 적절한 대책을 마련할 필요
  - 점검을 통해 파악된 문제점은 재발방지 대책을 포함해 개선조치 계획을 수립하고, CPO 및 개인정보 보호 부서는 개선조치가 계획대로 이행되었는지 최종 확인

개인정보 보호법(제31조)

제31조(개인정보 보호책임자의 지정 등) ⑤ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

CPO 체크리스트

- ☐ 내부 관리계획 이행 실태를 포함한 개인정보 처리 전반의 점검 계획을 체계적으로 수립하고 있는가?
- ☐ 점검 계획에 따라 점검을 수행하고 그 결과를 경영진에게 보고하고 있는가?
- ☐ 점검 결과 미흡사항에 대해 재발방지 대책을 포함한 개선조치 계획을 수립·이행하고 있는가?

관련 법령

- 법 제31조(개인정보 보호책임자의 지정 등) 제5항
- 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

3-9 개인정보파일 관리(공공기관 의무사항)

• 공공기관의 CPO는 개인정보파일을 체계적으로 관리하기 위한 절차를 마련하고 매년 1회 이상 일제 정비를 통해 최신성이 유지 될 수 있도록 관리·감독을 수행하여야 함

◆ 개인정보파일 관리 절차 수립

○ (절차 수립) 개인정보파일 생성, 변경, 파기 및 공개 등을 체계적으로 관리할 수 있도록 다음을 고려해 내부 절차 수립

절 차	주요내용	업무담당
1. 개인정보파일 식별	· 개인정보 처리 업무를 통해 생성되는 개인정보파일 식별 · 식별된 개인정보파일은 개인정보파일 등록 신청하고 CPO는 결재 및 승인 ※ 개인정보파일 등록 신청서 작성	업무처리 부서
⬇		
2. 개인정보파일 공개	· 개인정보 보호책임자는 60일 이내에 신규 개인정보보호파일을 intra.privacy.go.kr에 등록	개인정보 보호 부서
⬇		
3. 개인정보파일 대장 작성	· 개인정보파일 대장을 작성하여 개인정보파일을 체계적으로 관리 ※ intra.privacy.go.kr에 공개된 개인정보파일과 일치하도록 현행화	개인정보 보호 부서
⬇		
4. 개인정보파일 일제정비	· 개인정보파일은 연 1회 이상 일제정비를 통해 최신화 관리	개인정보 보호 부서
	· 기존 개인정보파일의 변경이 발생한 경우 개인정보파일 변경을 신청하고 CPO는 결재 및 승인 · 개인정보파일이 더 이상 사용되지 않아 파기를 수행할 경우 개인정보파일 파기를 요청하고 CPO의 결재 및 승인 후 개인정보파일 파기 관리대장에 기록 · 관리 ※ 개인정보파일 변경등록 신청서, 개인정보파일 파기 요청서, 개인정보파일 파기 관리대장 작성	사업 부서, 개인정보 보호 부서

개인정보파일 일제 정비

- (일제 정비) CPO는 연 1회 이상 개인정보파일 일제 정비를 통해 현행화 관리 필요

  ※ 비공개 대상의 개인정보파일도 내부적으로 식별하여 개인정보파일대장으로 관리하여야 함

일제 정비 시 점검사항

- ✓ 개인정보파일 대장에 누락된 개인정보파일이 없는지 확인
- ✓ 신규 개인정보파일이 없는지 확인
- ✓ 기존 개인정보파일에 처리근거, 수집항목, 제3자 제공 등 변경사항이 없는지 확인
- ✓ 개인정보파일이 더 이상 불필요하게 되어 파기대상이 없는지 확인
- ✓ 개인정보파일 중 개인정보 영향평가 대상이 없는지 확인

개인정보파일 등록 및 공개

- (등록 및 공개) CPO는 운용을 시작하는 날로부터 60일 이내에 해당 개인정보파일을 intra.privacy.go.kr에 등록하여 공개하여야 함

  – 다음의 비공개 대상의 개인정보파일은 등록 예외

개인정보파일 등록 예외

- ✓ 국가 안전, 외교상 비밀, 그 밖에 국가의 이익에 관한 사항을 기록한 개인정보파일
- ✓ 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
- ✓ 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
- ✓ 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일
- ✓ 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
- ✓ 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일
- ✓ 다른 법령에 따라 비밀로 분류된 개인정보파일

CPO 체크리스트

- □ 개인정보파일 관리를 위한 업무 절차를 마련하고 있는가?
- □ 개인정보파일 일제정비를 통해 현행화하여 관리하고 있는가?
- □ 개인정보파일 등록 및 공개 의무를 준수하고 있는가?

관련 법령

- 법 제32조(개인정보파일의 등록 및 공개)
- 영 제33조(개인정보파일의 등록사항 등)
- 표준 개인정보 보호지침 제4장 공공기관 개인정보파일 등록·공개

3-10 개인정보의 국외 이전 법적의무 관리

• CPO는 개인정보 흐름도를 통해 국외 이전의 현황 및 그 유형을 파악하고, 법상 국외 이전의 근거를 마련하여, 개인정보 처리방침 등을 통해 관련 내용을 공개하여야 함

◆ 국외 이전의 필요성 및 현황 검토

○ (흐름도 파악) CPO는 제공하는 모든 서비스에 대한 개인정보 처리의 국외 이전 흐름도 파악 필요

- (다수의 서비스 제공 시) 서비스별 카테고리를 구분하여 전체 서비스의 국외 이전 흐름을 파악하고 각 서비스별 흐름도를 개별 작성하는 방법 고려 가능

○ (유형 파악) 제공하는 서비스의 국외 이전 유형이 법상 제공(조회되는 경우를 포함) · 처리위탁 · 보관 중 어디에 해당하는지 유형 확인

(참고) 국외 이전이 아닌 경우

» 국외 사업자 등이 자사 개인정보 처리시스템을 통해 국내 정보주체의 개인정보를 직접 수집하는 경우는 법상 '국외 이전'에 해당하지 않음

【예시】 우리나라 정보주체를 대상으로 서비스를 제공하는 국외 사업자가 회원가입, 서비스 이용 시 우리나라 정보주체의 개인정보를 국외에 위치한 자사 시스템에서 직접 수집·처리하는 경우

◆ 국외 이전의 법적 근거 검토

○ (원칙적 금지) 법은 개인정보 국외 이전을 원칙적으로 금지

- (예외적 허용) CPO는 개인정보의 국외 이전을 위해 다음 중 하나의 법적 근거에 해당하는지 확인할 필요

① '국가(또는 국제기구)', 법률 등에 관한 적법한 근거 여부

✓ 이전되는 국가(또는 국제기구)의 개인정보 보호체계가 국내법과 실질적으로 동등한 수준임을 개인정보위가 인정하는 경우 및 법률, 조약 또는 국제협정에 따른 이전인지 확인(법 제28조의8제1항제2호, 제5호)

② '개인정보를 이전 받는 자'에 관한 적법한 근거 여부

✓ 개인정보를 이전받는 자가 ISMS-P 등 개인정보위가 고시하는 개인정보 보호 인증을 받았는지 확인 (법 제28조의8제1항제4호)

③ '국외 이전의 유형'에 따른 적법한 근거 여부

✓ 개인정보를 이전받는 자와의 관계에서 정보주체와의 계약의 체결 및 이행을 위하여 개인정보의 처리위탁 · 보관이 필요한 경우에 해당하는지 확인 (법 제28조의8제1항제3호, 제30조, 영 제29조의7)

④ '정보주체의 동의'에 따른 적법한 근거 여부

✓ 정보주체로부터 국외 이전에 관한 별도의 동의를 받았는지 확인(법 제28조의8 제1항제1호)

국외 이전 시 보호조치 등 검토

- (법령 준수) CPO는 국외 이전의 법적근거에도 불구하고 법의 개인정보의 제공, 목적 외 이용·제공 제한 및 개인정보를 제공받은 자의 이용 · 제공 제한 규정을 준수했는지 별도 검토 필요 (법 제28조의8 제4항, 법 제17조, 제18조, 제19조)
  - (국외 이전 시 보호조치) 개인정보 보호를 위한 안전성 확보 조치, 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치, 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 조치 등이 요구되므로 이에 대한 사전 검토 필요(법 제28조의8제4항, 영 제29조의10제1항)

- (법위반 계약 체결 금지) CPO는 개인정보의 국외 이전에 관한 계약에 법 위반 사항이 있는 검토 필요 (법 제28조의8제5항)
  - (계약내용 반영) 이전받는 자와 국외 이전의 예외적 허용 중 어느 하나에 해당하는지 사전 협의하고 이를 계약내용 등에 반영하였는지 검토(법 제28조의8제4항, 영 제29조의10제2항)

국외 이전에 따른 공개 사항 확인

- (공개 사항) CPO는 개인정보의 국외 이전 시 이전 유형과 관계없이 아래 사항이 개인정보 처리방침에 공개되었는지 확인할 필요
  (법 제28조의8 제2항, 법 제30조 제1항 제8호, 영 제31조 제1항)

국외 이전 관련 개인정보 처리방침 공개 사항

- ✓ 국외 이전 법적 근거
- ✓ 이전되는 개인정보 항목
- ✓ 개인정보가 이전되는 국가, 시기, 방법
- ✓ 개인정보를 이전받는 자의 성명
- ✓ 개인정보를 이전받는 자의 개인정보 이용목적 및 보유 · 이용기간
- ✓ 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과

※ 이는 국외 재이전의 경우에도 동일하게 적용됨(법 제28조의11)

※ (국외 이전이 아닌 경우 공개 사항) '국외에서 국내 정보주체의 개인정보를 직접 수집하여 처리하는 경우'는 국외 이전에는 해당하지 아니하나 개인정보를 처리하는 국가명을 개인정보 처리방침에 공개해야 함(영 제31조 제1항제4호)

중지명령 대응 등 위험관리

- (중지 명령) 개인정보위는 개인정보처리자가 개인정보를 국외 이전하는 과정에서 법령 위반, 적절한 개인정보 보호 조치를 취하지 않아 정보주체에게 피해가 발생하거나 발생할 우려가 있는 경우 국외 이전을 중지하도록 명령할 수 있음(법 제28조의9, 영 제29조의11)
  - CPO는 국외 이전 중지 명령으로 서비스 제공 자체가 제한될 수 있는 상황을 고려하여, 국외 이전 과정에서의 개인정보 관련 법령 준수, 피해발생 가능성을 지속적으로 점검할 필요
  - 국외 이전 중지에 따른 비즈니스 영향도를 경영진 및 해당 부서에 사전에 충분히 알리고 인식 제고를 위해 노력하여야 함

- (위험평가 및 관리) 글로벌 지정학적 이슈에 따른 서버 위치 변경, 개인정보위의 동등성 평가, 이전받는 자의 보호수준의 변경 등 위험이 지속적으로 변경될 가능성 존재
  - CPO는 국외 이전 관련 위험관리 절차를 구축하여 정보주체 보호, 지속가능한 글로벌 서비스 제공 등이 가능하도록 관리할 필요

CPO 체크리스트

- ☐ 개인정보처리자가 제공하는 서비스에 관한 국외 이전(재이전 포함) 흐름을 파악하고 있는가?
- ☐ 개인정보 국외 이전에 관한 적법한 근거를 분석하고 해당여부를 확인하고 있는가?
- ☐ 국외 이전에 관해 공개할 내용을 개인정보 처리방침에 공개하고 있는가?
- ☐ 국외 이전 시 보호조치를 마련하고 있는가?
- ☐ 중지명령, 지정학적 이슈, 동등성 평가 등 국외 이전 관련 위험에 대응하기 위한 프로세스를 마련하고 있는가?

관련 법령

- 법 제28조의8(개인정보의 국외 이전)
- 법 제28조의9(개인정보의 국외 이전 중지 명령)
- 법 제28조의10(상호주의)
- 법 제28조의11(준용규정)
- 법 제30조(개인정보 처리방침의 수립 및 공개)
- 영 제29조의7(개인정보 국외 처리위탁 · 보관 시 정보주체에게 알리는 방법)
- 영 제29조의8(개인정보 국외 이전 인증)
- 영 제29조의9(국가 등에 대한 개인정보 보호 수준 인정)
- 영 제29조의10(개인정보의 국외 이전 시 보호조치 등)
- 영 제29조의11(국외 이전 중지 명령의 기준)
- 영 제31조(개인정보 처리방침 내용 및 공개방법 등)

4 개인정보 활용 안전조치 및 관리감독

4-1 개인정보 위험관리 체계 구축·점검

• CPO는 개인정보 침해 위협에 대응하여 개인정보 처리에 수반되는 위험을 식별하고 평가하여 적절한 대책을 마련하고 자원을 효율적으로 배치 · 활용하는 등 개인정보 위험을 체계적으로 관리할 필요가 있음

위험관리 정의 및 필요성

○ (정의) 개인정보 위험관리는 개인정보 처리에 따른 관련 위험을 지속적으로 평가하고, 효과적이고 효율적인 보호대책을 마련하는 일련의 과정을 의미함

- 법령 등에서도 정보주체의 권리침해 가능성과 위험 정도를 고려하여 개인정보를 안전하게 관리하도록 안내하고 있음

위험관리 관련 법제도

① **개인정보 보호법**

- **제3조(개인정보 보호 원칙)** ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

② **개인정보의 안전성 확보조치 기준**

- **제3조(안전조치의 적용 원칙)** 개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용하여야 한다.
- **제4조(내부 관리계획의 수립·시행 및 점검)** ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립 · 시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인 · 개인 · 단체의 경우에는 생략할 수 있다.

  13. 위험 분석 및 관리에 관한 사항

○ (필요성) 개인정보 보호 법규를 준수하여 법적 제재 리스크를 최소화하고 고객 신뢰 확보 및 비즈니스 연속성 보장 등을 위해 위험관리 필요

◈ 개인정보 위험관리 체계 구축·점검

- (위험관리 계획) CPO는 조직의 환경에 맞는 개인정보 위험평가 절차 및 관리 계획을 수립·이행
- (위험식별) 체계적인 개인정보 위험관리를 위해 조직의 개인정보 처리에 대해 어떠한 위험들이 존재하는지 명확하게 식별

개인정보 위험 예시

- ✓ 개인정보의 기밀성 손상(개인정보의 분실, 도난, 유출 등)
- ✓ 개인정보의 무결성 손상(개인정보의 위조, 변조 등)
- ✓ 개인정보의 가용성 손상(개인정보의 훼손 등)
- ✓ 개인정보 생명주기별 처리의 적법성 미흡
- ✓ 개인정보 파기 미흡
- ✓ 정보주체 권리보장 미흡
- ✓ 개인정보취급자에 의한 개인정보 오·남용
- ✓ 개인정보 처리 원칙 위배 등

- (위험분석) 개인정보 영역의 특성(법적 준거성, 정보주체 권리 침해 등), 개인정보 생명주기 단계(개인정보의 수집, 저장, 이용·제공, 파기 등) 등을 고려하여 위험을 분석
  - (위험평가 및 관리) 위험분석 결과를 바탕으로 수용가능한 위험수준 결정 및 수용가능한 위험수준을 초과하는 위험에 대해서는 적절한 대책을 수립 · 이행
- (점검 및 환류) 개인정보 위험은 관련 법규의 개정, 신기술 도입 등 대내외 환경에 따라 변화하는 특성이 있으므로, CPO는 정기·비정기적으로 개인정보 위험을 평가·관리
  - (정기적 관리) 연 1회 이상 정기적인 위험평가를 통해 기존 위험의 변화 여부, 새로운 위험의 출현 여부 등의 평가 및 대책 수립
  - (비정기적 관리) 신규 서비스 출시, 개인정보처리시스템 개발·변경 등에 따라 개인정보 처리에 따른 위험변화가 예상되는 경우에는 해당 처리가 이루어지기 전에 개인정보 영향평가 등을 수행

CPO 체크리스트

- □ 개인정보 위험을 체계적으로 식별·평가할 수 있도록 조직의 환경에 맞는 위험평가 절차가 마련되어 있는가?
- □ 위험평가 절차에 따라 정기적 및 비정기적으로 개인정보 위험을 평가하고 있는가?
- □ PDCA(Plan-Do-Check-Act) 관점에서 개인정보 위험을 지속적으로 관리하고 있는가?

관련 법령

- 법 제3조(개인정보 보호 원칙)
- 법 제33조(개인정보 영향평가)
- 개인정보의 안전성 확보조치 기준

참고자료

- 개인정보의 안전성 확보조치 기준 안내서(개인정보위, 2024.10.)
- 개인정보 영향평가 수행안내서(개인정보위, 2024.4.)
- ISMS-P 인증기준 안내서(과기정통부·개인정보위·KISA, 2023.11.)

4-2 개인정보 보호 중심 설계(PbD, Privacy by Design)

• CPO는 개인정보 처리에 수반되는 새롭고 다양한 위험에 효과적 · 선제적으로 대응할 수 있도록 개인정보 보호 중심 설계 원칙(PbD)을 확립하고 조직에 적합한 절차를 수립 · 이행할 필요가 있음[4)]

PbD 정의 및 체계

- (정의) 제품 또는 서비스의 기획, 제조, 폐기 등 전 과정에서 개인정보 보호 요소를 충분히 고려함으로써 개인정보 침해를 사전에 예방하는 설계 개념[5)]
  - 개인정보 보호는 침해 발생 이후 대응하는 것보다 기획 · 설계 단계에서 개인정보 침해 요인을 예측하고 사전 예방하는 것이 효율적
  - 인공지능 등 IT 환경에 급격히 변화함에 따라 침해 유형과 기법도 고도화·지능화되고 있어 개인정보 보호 중심 설계 중요성 부각

| Privacy by Design 7대 원칙 |

구분	원 칙	설 명
1	사후 조치가 아닌 사전 예방 (Proactive not reactive – preventive not remedial)	· 프라이버시 침해가 발생한 뒤 조치가 아닌 침해를 예상하고 조치
2	기본 설정으로 프라이버시 보호조치 (Lead with privacy as the default setting)	· 사용자가 별도 조치하지 않아도 프라이버시가 자동으로 보호되도록 기본 설정
3	프라이버시 보호를 설계에 내재화 (Embeded privacy into design)	· 프라이버시 보호를 제품·서비스·시스템 등의 설계에 내재화
4	완전한 기능성 유지 – 제로섬이 아닌 포지티브섬 (Retain full functionality – positive-sum, not zero-sum)	· 개인정보 보호와 비즈니스 목적을 동시에 달성할 수 있도록 상호 배타적이지 않은 방법 고려
5	개인정보 생애주기 전체에 대한 보호 (Ensure End-to-End security)	· 개인정보의 수집·이용·저장·제공·파기 등 모든 단계에 안전조치를 적용
6	개인정보 처리 과정에 대한 가시성 및 투명성 유지 (Maintain visibility and transparency – keep it open)	· 개인정보 처리 및 보호 방안을 투명하게 공개하여 이해관계자가 쉽게 확인할 수 있도록 보장
7	정보주체 프라이버시 존중 (Respect user privacy – keep it user centric)	· 사용자 중심으로 시스템과 절차를 설계하고 개인정보와 관련된 선택과 통제를 사용자에게 부여

※ 출처 : Ann Cavoukian

4) PbD도 개인정보 위험(risk) 관리 중 비정기적 관리의 한 방법으로 볼 수 있음

5) 캐나다 온타리오주 프라이버시 커미셔너 앤 카부키안(Ann Cavoukian) 박사가 Privacy by Design이란 개념으로 1990년도 중반에 처음 소개하였으며, EU GDPR를 비롯하여 국제적으로 광범위하게 통용되는 개인정보보호 원칙

| PbD 절차 예시 |

구분	서비스 생애주기	PbD 활동
1	서비스 기획	· 서비스 기획 단계에서부터 개발, 운영 단계 전반에 개인정보 보호 조직이 함께 참여할 수 있도록 정책 및 공식적인 절차 마련 · 서비스 특성을 고려한 개인정보 위험요인 최소화 방안 도출(개인정보 처리의 적법성 근거 및 안전한 활용 방식 마련 등) · 필요 시, 기획단계 간이 개인정보 영향평가 수행 등 ※ 비즈니스 및 서비스를 이해하고, 비즈니스적인 기능과 편의성, 보안성, 개인정보 보호를 동시에 달성할 수 있는 방안 고려 필요
2	분석·설계	· 개인정보 보호 관련 요구사항 도출 · 서비스 흐름 및 개인정보 흐름 분석(위험분석 포함) · 개인정보 보호 기본 설정(Privacy by Default)을 포함하여 개인정보 보호조치 내재화 설계 · 개인정보 영향평가 수행 및 개선과제 도출 등 ※ 서비스 흐름 및 시스템 내에 개인정보 보호조치를 내재화할 수 있는 방안 고려 필요
3	구현	· 이전 단계에서 마련된 개인정보 보호 조치 설계에 따라 개발 수행 · 개인정보 영향평가 개선과제에 대한 이행 · 개발보안 절차 이행 등
4	테스트	· 개인정보 보호조치 설계가 서비스 및 시스템에 적절히 적용되었는지 여부에 대한 테스트 및 검증 · 보안취약점 점검 · 개인정보 영향평가 개선과제에 대한 이행점검 등
5	운영	· 개인정보 보호조치의 효과성 점검 · 개인정보 위험에 대한 주기적 평가 · 개인정보 처리방법, 흐름 등의 변경이 발생할 경우, PbD 활동의 반복 수행 · 서비스 종료시 개인정보 보호조치 수행 및 점검 등

- (PbD 체계 구축) PbD는 개인정보 처리와 관련된 위험에 대응하기 위한 선제적 방안이 될 수 있으므로, CPO는 조직 내 PbD 원칙을 확립하고 조직의 환경에 맞는 PbD 체계 구축 검토
  - 서비스 특성, 개발 절차, 가용자원, 개인정보 처리에 따른 위험도 등을 확인하고, 새로운 개인정보의 처리가 이루어지기 전에 최대한 빠른 시기부터 논의 착수

PbD 적용 절차 예시

- ✓ 수집·이용 등 처리하려는 데이터 현황 파악
- ✓ 개인정보 항목과 유형(식별자, 속성정보 등) 분석
- ✓ 개인정보 처리 흐름 분석
- ✓ 개인정보 처리에 따른 위험성·침해요인 분석
- ✓ 개인정보 항목별 수집 근거(동의, 계약 체결·이행 등)와 활용 방식(가명처리 등) 결정
- ✓ 개인정보 보호조치 선정 및 적용방안 마련

- (유관부서 협업) 사업부서, 개발부서 등 유관부서와 함께 개인정보 보호 조치의 내재화 방안을 논의하고 PbD 관련 상호 협력체계를 조성함으로써 업무 효율화 기반 마련

◆ PbD 구현방안

- (PbD 적용) CPO는 PbD 원칙의 효과적인 적용을 위하여 서비스 전반의 개인정보 처리 관련 사항을 검토하고 최적의 보호조치를 선정하여 이를 서비스 및 시스템에 내재화하는 방식으로 적용
  - (PbD에 따른 개인정보 보호조치) 개인정보 처리의 적법성 확보, 가명·익명처리, 개인정보 보호 기본 설정(Privacy by Default), 개인정보 보호 강화기술(PET, Privacy Enhancing Technology[6]) 적용 등

AI 관련 PbD 원칙을 적용한 보호대책 예시

- ✓ AI 라이프 사이클별 보호 원칙·기준 마련
- ✓ 개인정보 수집·이용 등 처리근거 명확화 및 적법성 확보
- ✓ 프라이버시 침해 방지를 위한 안전성 확보조치 등 대응계획 마련
- ✓ 데이터 오류·편향·왜곡 및 차별과 편견 최소화 방안 마련·이행
- ✓ 학습데이터 출처, 개인정보 처리방법 등의 공개방안 마련·이행
- ✓ 정보주체 권리보장 방안 및 소통·신고처리 창구 구축·운영계획 마련
- ✓ 위험, 침해요인 등을 파악하고 대응조치를 설계-적용-관리하는 거버넌스 체계 구축

※ 출처 : 인공지능 시대 안전한 개인정보 활용 정책방향(개인정보위, 2023.8.)

6) PET란 개인정보 침해위험을 효과적으로 관리하면서도 개인정보의 안전한 활용을 지원하기 위한 기술로서 차분 프라이버시(Differential Privacy), 동형암호화, 합성데이터 등이 이에 해당됨

○ (개인정보 영향평가) 개인정보 영향평가(PIA; Privacy Impact Assessment)는 PbD 원칙 적용의 실질적인 역할 수행 가능

개인정보 영향평가

- (정의) 개인정보 영향평가란 개인정보 처리로 인한 잠재적인 개인정보 침해 발생 가능성 및 영향을 사전에 조사 · 예측 · 검토하여 개선방안을 도출하는 체계적인 절차
- (효과) 개인정보 영향평가를 통해 서비스 및 시스템 기획·분석·설계 단계에서 PbD 요소를 도출하고, PbD 적용을 위한 방안을 마련할 수 있음
  - 공공기관의 경우 법 제33조에 따라 법적 요건에 해당되는 개인정보파일을 구축·운용하려는 경우에는 설계 완료 전에 개인정보 영향평가를 의무적으로 수행해야 함
  - 공공기관 외 개인정보처리자의 경우 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 함

○ (영향평가 수행·관리) CPO는 조직, 서비스 특성 등을 고려하여 개인정보 영향평가 수행 기준, 세부 수행절차, 수행방법, 점검항목 등을 정의하고 지속적으로 관리
  - (공공기관) '개인정보 영향평가 수행안내서(개인정보위, 2024.4)'를 참고하여 수행절차 마련
  - (공공기관 외 개인정보처리자) '개인정보 영향평가 수행안내서(개인정보위, 2024.4.)', ISO/IEC 29134 등 국내·외 표준을 참고하여 조직 환경에 최적화된 개인정보 영향평가 수행 기준 및 절차 마련

영향평가 필요성 검토 결과에 따른 영향평가 수행 기준 예시

- ✓ 높은 위험이 예상될 경우, 정식 영향평가 수행
- ✓ 중간 위험이 예상될 경우, 간이 영향평가 수행
- ✓ 낮은 위험이 예상될 경우, 영향평가 생략 또는 체크리스트 기반의 자가검토 수행 등

| 개인정보 영향평가 단계별 절차 예시 및 CPO 주안점 |

단계	구분	설명	CPO 주안점
사전 준비 단계	영향평가 필요성 검토 및 사업계획 작성	· 개인정보파일의 신규 구축, 변경 시 영향평가 수행 필요성 검토(법적 요건, 위험도 등 고려) · 영향평가 예산 확보 · 영향평가 기관 선정 등	· 영향평가 필요성 검토를 위한 기준 및 절차의 수립·이행 · 사업 추진시 영향평가 필요성 검토절차가 누락되지 않도록 절차 및 방안 마련 필요(구매 절차 연계 등)
영향평가 수행 단계	평가계획 수립	· 평가수행 계획 수립 및 평가팀 구성	· 영향평가의 주안점 및 방향을 명확히 지시 · 영향평가 대상 서비스 및 시스템에 특화된 위험이 식별되고, PbD가 적용될 수 있도록 위험평가 방법 및 평가지표 등 정의 · 영향평가가 충실히 수행될 수 있도록 보고 및 의사소통체계 마련(주요 사항은 반드시 CPO에게 보고 필요) · 평가팀 구성 지원(유관 조직 및 유관 담당자의 참여 등) · 위험도 산정 후 위험조치 및 수용 여부에 대한 최종 의사결정 · 영향평가서에 대한 최종 검토 및 결재
	평가자료 수집	· 내부 자료, 외부 자료, 대상 시스템 관련 자료 수집 및 분석	
	개인정보 흐름분석	· 개인정보 처리업무 분석 및 업무 흐름도 작성 · 개인정보 흐름표 및 흐름도 작성 · 시스템 구조도 작성	
	개인정보 침해요인 분석	· 평가항목 작성 · 개인정보 보호조치 현황 파악 · 개인정보 침해요인 도출 및 위험도 산정	
	개선계획 수립	· 개선사항 도출 · 개선계획 수립	
	평가보고서 작성	· 영향평가서 및 요약서 작성 · 공공기관의 경우, 영향평가서 제출	
이행 단계	개선계획 반영·점검	· 개선계획 반영(개발단계) · 개선계획 반영점검(테스트단계)	· 개선계획이 실질적으로 이행될 수 있도록 관리(개발 조직과 유기적 협조체계, 이행점검 절차 마련 등) · 중장기 개선과제에 대한 지속적인 이행 관리
	개선계획 이행확인	· 개선사항 이행확인 · 공공기관의 경우, 이행확인서 제출	

CPO 체크리스트

□ 조직의 특성에 맞는 PbD 정책 및 절차를 마련하였는가?

□ PbD 절차가 효과적으로 이행될 수 있도록 관련 조직간의 R&R을 명확히 정의하였는가?

□ 개인정보 영향평가 필요성 검토 절차 및 수행체계(기준, 방법론, 조직, 인력 등)가 마련되어 있는가?

관련 법령

- 법 제3조(개인정보 보호 원칙)
- 법 제33조(개인정보 영향평가)
- 개인정보 영향평가에 관한 고시

참고자료

- 개인정보 영향평가 수행안내서(개인정보위, 2024.4.)

4-3 가명정보 관리·감독

• 데이터 3법 개정에 따라 정보주체 동의 없이 개인정보를 안전하게 활용할 수 있는 가명정보 제도가 도입되었으므로, CPO는 전사적인 데이터 거버넌스를 고려하여 가명정보 관리체계를 수립하고 가명정보의 안전한 활용을 지원·촉진할 필요가 있음

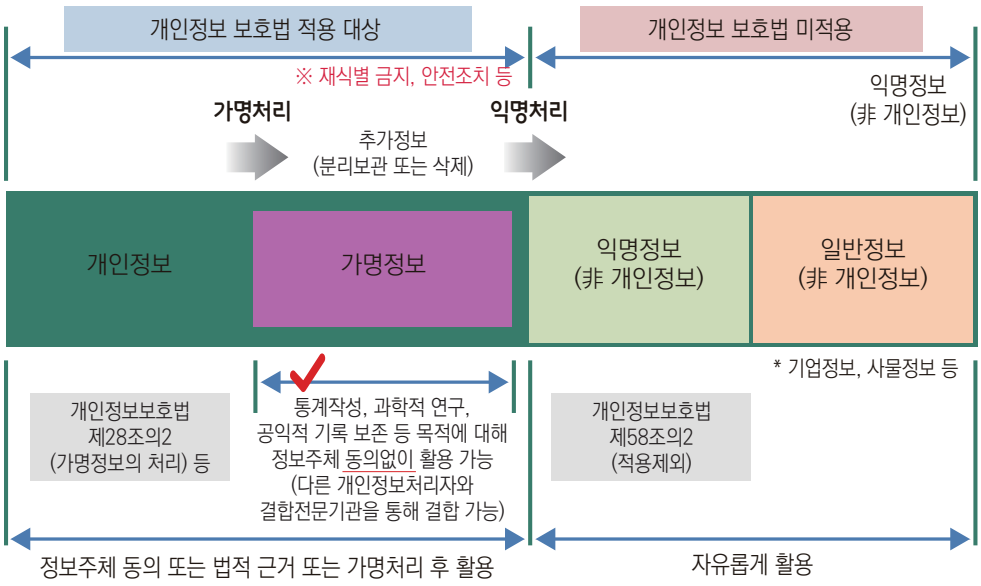
정의 및 활용범위

○ (가명정보) 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가적인 정보가 없이는 특정 개인을 알아볼 수 없도록 가명처리를 거쳐 생성된 정보를 의미

– (활용범위) 통계작성, 과학적 연구, 공익적 기록보존 등의 목적에 한해 정보주체 동의없이 분석·활용·제공 등 처리 가능

※ 다만, 추가정보의 분리보관 또는 삭제, 접근 권한의 분리, 가명정보 처리기록의 보관, 가명정보 처리기간 설정 및 파기, 개인정보 처리방침 공개 등 가명정보에 대한 안전조치 의무 이행 필요

| 가명정보 처리의 개념 |



○ (가명정보 활용) 통계작성, 과학적 연구, 공익적 기록보존 등을 위해 서로 다른 개인정보처리자 간의 가명정보 결합·활용이 가능하며, 가명정보 결합은 결합전문기관*을 통해 실시

* 개인정보위 또는 관계 중앙행정기관의 장이 지정하는 기관을 활용할 수 있으며, 가명정보의 결합과 관련된 사항은 가명정보 지원 플랫폼(dataprivacy.go.kr) 참고

- (가명정보 활용지원) 가명정보 지원 플랫폼 및 주요 지역별로 운영 중인 가명정보 활용 지원센터를 통해 가명정보 처리관련 컨설팅·기술지원, 교육·훈련·실습 등을 지원을 받을 수 있음
- (개인정보 안심구역) 개인정보위에서 지정하는 '개인정보 안심구역'이용 시, 안전한 처리 환경 하에서 기존에 사실상 제한되어 왔던 다양한 가명정보의 처리 가능

개인정보 안심구역 주요 기능

✓ (PET 실증) 동형암호화, 합성데이터, 차분 프라이버시 등 기존 규제적용이 모호한 PET(개인정보 보호 강화기술)에 대해 전문심의위가 실증계획을 검증하여 충분한 안전성을 확보했다고 판단한 경우, 해당 기술을 적용한 개인정보 처리 허용

✓ (비정형데이터 활용) 비정형데이터는 가명처리 적정성 육안 전수검사에 막대한 시간·비용이 소요되므로 전문심의위가 검증한 가명처리 SW를 적용하면 샘플링 검사 후 활용 허용

✓ (가명처리 수준 완화 등) 가명처리 수준을 적정 수준으로 완화, 다양한 결합키 활용을 통해 결합률 제고, 인공지능(AI) 개발, 시계열 분석 등 지속적·반복적 연구를 위한 가명정보의 장기간 보관 및 제3자 재사용 가능 등

○ (활용 관련 가이드라인) 가명정보 처리와 관련된 절차, 방법 등 세부사항은 가명정보 처리 가이드라인을 비롯하여 보건·의료, 교육, 공공, 금융 등 분야별 가이드라인을 참고할 수 있음

가명정보 성과 및 조직 내 관리체계

- (성과사례) 가명정보 제도를 잘 활용할 경우 법적 허용범위 내에서 개인정보의 안전한 활용을 통해 다양한 성과창출 가능

가명정보 활용 성과 사례

- ✓ 중소기업중앙회 공제·납부정보, 금융결제원 자동이체 정보, 신용정보 등 금융 및 비금융 정보의 가명결합을 통한 소상공인 신용평가모형 개발
- ✓ 척추전문 한방병원의 가명정보와 건강보험심사평가원 청구자료의 가명결합을 통한 척추질환 환자의 한방의료 이용에 따른 차이 분석
- ✓ 병원 데이터 및 국민건강보험공단 데이터의 가명결합을 통한 알코올 중독환자의 정신과적 치료에 대한 효과성 분석
- ✓ 에너지 복지 실태조사 및 에너지 사용량 데이터의 가명결합을 통한 에너지 복지 사각지대 분석 등

- (가명정보 관리체계) CPO는 조직 내에서 가명정보를 안전하고 효과적으로 활용할 수 있도록 가명정보 관리체계를 수립할 필요가 있음
  - 가명정보 처리 절차는 가명정보 처리 가이드라인의 절차를 참고하여, 데이터 처리 환경 및 분야 등 조직의 특성에 따라 가명처리절차를 마련

| 가명정보 처리 절차 예시 및 CPO 주안점 |

구분	설명	CPO 주안점
목적 설정 등 사전준비	· 법에서 정한 3가지 목적(통계작성, 과학적 연구, 공익적 기록 보존) 중에서 가명정보 처리의 목적을 구체적이고 명확하게 설정 · 처리 목적 달성에 필요한 정보의 종류, 범위 등 가명처리 대상 선정 · 처리 목적의 적합성 검토 · 가명정보 처리를 위한 안전조치 이행 (가명정보 처리에 관한 내부 관리계획 수립 등) · 필요 서류 작성 등(가명정보 처리 위탁 시 위탁계약서 작성 등)	· 조직 내 가명정보 처리 및 보호 담당자 지정 · 담당자 교육·훈련 등 역량 강화 · 사전에 가명정보 처리 기준, 절차, 조직간 R&R, 안전조치 사항 등을 규정한 가명정보 내부 관리계획 수립(기존 개인정보 내부 관리계획에 포함 또는 별도 문서로 마련) ※ 전사 데이터 거버넌스 차원에서 접근 필요
처리 대상의 위험성 검토	· 가명처리 대상 개인정보파일 및 개인정보 항목 선정 · 가명처리 대상 데이터의 위험성 검토 ① 데이터 자체 식별 위험성 : 식별정보, 식별가능정보, 특이정보, 재식별 시 영향도 등 ② 처리 환경 식별 위험성 : 활용 형태(내부 활용, 외부 제공, 외부 결합 등), 처리 장소, 처리 방법	· 내부 데이터 특성을 고려하여 주요 데이터 항목별 위험성 기준 마련 · 처리환경의 안전성이 높아질수록 양질의 가명정보 활용이 가능할 수 있으므로 안전한 가명정보 처리 환경 마련
가명처리	· 식별 위험성 검토 결과를 기반으로 가명정보의 활용 목적 달성에 필요한 가명처리 방법 및 수준을 정하여 항목별 가명처리 계획 설정 · 항목별 가명처리 계획을 기반으로 가명처리 수행 · 가명처리 과정에서 생성되는 추가 정보는 원칙적으로 파기하고 필요한 경우 가명정보와 분리하여 별도로 저장	· 추가정보의 안전한 생성, 이용, 보관, 파기 기준 마련 · 추가정보 담당자 지정
적정성 검토	· 가명처리에 대해 결과 적정성을 최종 검토 · 가명처리 적정성 검토는 내부 인원을 활용하여 자체적으로 검토하거나, 외부 전문가를 통하여 검토 가능(단, 최소 3명 이상으로 검토위원회를 구성하는 것을 권고) · 적정성 검토 결과 부적정으로 판단될 경우 추가 가명처리 후 다시 적정성 검토 수행	· 위험에 근거한 적정성 검토 절차 마련(예를 들어, 고위험 시 외부 위원 구성, 저위험 시 자체 검토 등) · 적정성 검토위원회 구성(분야별 내외부 전문가 섭외, CPO가 위원 또는 위원장으로 참여 가능) ※ 가명정보 처리의 목적이 안전한 활용에 있으므로, 지나치게 유용성이 떨어지지 않도록 균형 유지 필요
안전한 관리	· 사전준비 단계에서 수립한 내부 관리계획에 따라 가명정보에 대한 안전조치 의무 이행(추가정보 분리 보관 또는 삭제, 접근권한 분리 등) · 재식별 금지 및 재식별 가능성 점검 · 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기 · 가명정보 처리 관련 기록 작성 및 보관 · 가명정보 처리에 관한 사항을 개인정보 처리방침에 공개 · 가명정보 처리기간 종료 시 파기 등	· 가명정보 안전조치 담당자 지정 · 가명정보취급자 지정 및 관리·감독 · 가명정보 안전조치 이행 여부에 대한 정기적인 실태점검 · (필요 시) 가명정보 관리체계 개선 등

CPO 체크리스트

- □ 가명정보 처리 절차, 안전조치 기준, 조직간 R&R 등을 포함하는 가명정보 내부 관리계획을 조직의 특성에 맞게 수립하였는가?
- □ 가명정보 전문가 육성, 교육 등 내부역량 강화를 위한 방안이 마련되어 있는가?
- □ 가명정보를 처리하는 경우 가명정보 내부 관리계획의 이행실태를 정기적으로 점검하고, 문제점 발견 시 개선조치를 이행하고 있는가?

관련 법령

- 법 제28조의2(가명정보의 처리 등)
- 법 제28조의3(가명정보의 결합 제한)
- 법 제28조의4(가명정보에 대한 안전조치의무 등)
- 법 제28조의5(가명정보 처리 시 금지의무 등)
- 법 제28조의7(적용범위)

참고자료

- 교육분야 가명·익명정보 처리 가이드라인(교육부·개인정보위, 2024.8.)
- 합성데이터 생성 참조모델(개인정보위, 2024.5.)
- 가명정보 처리 가이드라인(개인정보위, 2024.2.)
- 보건의료데이터 활용 가이드라인(보건복지부·개인정보위, 2024.1.)
- 금융분야 가명·익명처리 안내서(금융위원회·금융감독원, 2022.1.)
- 공공분야 가명정보 제공 실무안내서(행안부·개인정보위, 2021.1.)

4-4 신기술 트렌드 분석 및 대응 방안 마련

• CPO는 인공지능 등 신기술 도입 개발·도입에 따른 개인정보 위험을 PbD, 개인정보 영향평가 등을 통해 선제적으로 대응할 필요가 있음

◈ 신기술 개인정보 위험 및 AI 위험 대응

○ AI 위험 대응

– (내부 관리체계 마련) AI · 데이터 처리의 적법성, 안전성 등을 확보할 수 있도록 CPO를 중심으로 '(가칭)AI 프라이버시 담당조직'을 자율적으로 구성 · 운영하는 것이 바람직

(가칭)AI 프라이버시 담당조직의 역할

✓ 학습데이터 수집 · 이용의 적법성을 포함하여 AI · 데이터 처리 전반의 개인정보 보호법 준수를 확보

✓ AI 성능 개선 등 중대한 기술적 변경이나 개인정보 침해 발생 우려 등 리스크 요인을 주기적으로 모니터링

✓ AI 개발 · 운영 과정에서 개인정보 유 · 노출 등 침해사고가 발생할 경우 신속히 권리구제 방안을 마련 · 안내하고 정보주체 권리행사를 적극적으로 지원

– (AI 프라이버시 보호 문화 공유 및 확산) AI 프라이버시 위험에 대한 점검 · 평가 결과 및 개선조치에 대해 CPO가 기관 내부 구성원과 공유하고 교육 · 홍보 강화도 병행하여 AI 프라이버시 보호 문화가 기관 내부에 확산될 수 있도록 노력

〈참고〉 인공지능 라이프 사이클에 따른 주요 위협요인 및 대책 예시[7]

구분	인공지능 라이프 사이클(AI Lifecycle)			
	① 데이터 수집	② 데이터 저장·전처리	③ 데이터 학습·모델링·검증	④ AI 서비스 제공
주요 위협 요인	· 개인정보 수집의 적법 요건 위반 · 공개된 개인정보 수집의 적법성 미흡 · 과도한 개인정보 수집(민감정보, 아동의 개인정보 포함 등) · 영상정보처리기기, IoT 센서 등 자동수집 장치를 통한 개인정보 수집시 개인정보 수집의 적법성 미확보	· 저장된 개인정보의 유·노출, 훼손, 변조 · 불완전한 가명처리·익명처리에 따른 개인정보 재식별 · 개인정보처리시스템(빅데이터 플랫폼 등)에 대한 안전성확보조치 기준 위반 등	· AI 학습을 위한 개인정보 처리의 적법 요건 위반 · 학습 과정에서 민감정보 추론 가능성 발생 · 개인정보 재식별 또는 유출 등 · AI 모델에 특화된 취약점 발생 등	· 서비스 레벨 개인정보 침해 이슈(해킹 또는 프로그램 오류 등에 따른 회원정보 및 대화정보 유·노출 등) · AI 모델 특화 취약점 공격(학습데이터 추출 또는 추론 등) · 정보주체 권리 보장 미흡(자동화된 결정에 대한 거부 및 설명요구 등)
주요 대책	· 적법 요건 식별 및 준수(동의, 법률 또는 법적 의무, 계약 이행 등) · 데이터 출처 확인 및 관리 · 실시간 익명처리 등	· 적정수준의 개인정보 가명처리·익명처리 · 개인정보처리 시스템에 대한 안전성 확보조치 적용 · 데이터 백업 등	· 적정수준의 개인정보 가명처리·익명처리 · 보안 및 프라이버시 이슈에 강건한 AI 모델 개발 · 개인정보 재식별 가능성, 민감정보 추론 가능성 등에 대한 검증 및 필터링 등	· 개인정보 안전조치 강화 · 개인정보 재식별 가능성 점검 · 보안 및 프라이버시 이슈에 강건한 AI 모델 개발 · AI 서비스 정보주체 권리보장 방안 마련 등
관련 보호 기술 (PET 등)	· 연합 학습 · Local Differential Privacy(LDP) · Edge Computing · 개인정보 검색 및 필터링 · 합성데이터 등	· 가명처리·익명처리 기술(DP 등) · 합성데이터 · 암호기술 · 백업기술 · 접근통제 등 보안기술	· 가명처리·익명처리 기술(DP 등) · 암호기술(동형암호화 등) · 연합 학습 · MPC · 접근통제 등 보안 기술	· XAI(Explainable AI) · 머신 언러닝 · API 및 Plug-in 보안 · 해킹 등 침해대응 보안기술 등

7) 출처 : AI PET 보고서(개인정보 기술포럼, 2024.1)

◎ (사전적정성 검토제도 활용) 신기술이 적용된 새로운 서비스의 도입·개발과 관련하여 법규 준수의 어려움 등 높은 위험이 존재하는 경우, 개인정보위가 운영 중인 사전적정성 검토제를 활용할 수 있음

- (정의) 사전적정성 검토제란 AI 등 신기술 개발이나 신규 서비스 제공을 기획하는 과정에서 법을 준수하는 방안을 사업자와 정부가 함께 마련하고, 사업자의 신청에 따라 사전 적정성 검토의견서에 적정하다고 판단하여 회신한 경우 해당 행위에 대해 행정처분 대상에서 제외하는 제도임

사전적정성 검토제 운영규칙 주요 내용

✓ (신청대상) 개인정보 처리가 아직 개시되지 않은 신서비스·신기술

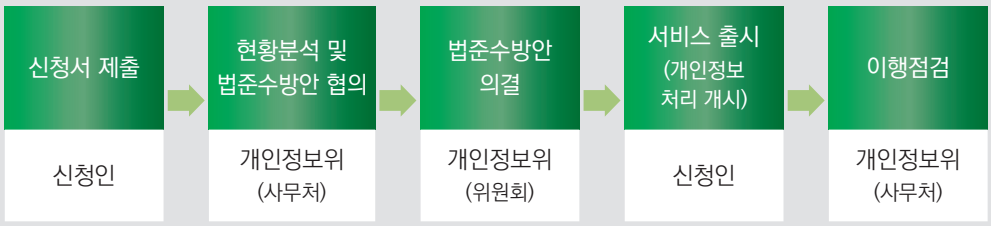
✓ (접수기준) '법령이 개정되어야만 신청 대상 서비스가 적법하게 될 수 있다' 등의 특별한 사정이 없는 한 사전적정성 검토 신청을 수리

✓ (검토(안) 마련) 개인정보위 소관부서와 신청인이 협의 하에 대상 서비스 현황을 분석하고, 법 준수방안을 함께 마련

✓ (심의·의결) 개인정보위 전체회의 또는 소위원회 심의·의결을 거쳐 사전적정성 검토결과를 신청인에게 회신

✓ (사후대응) 회신 이후 신청인이 협의된 준수방안에 따라 적정하게 서비스를 제공하는지 개인정보위가 점검, 최종적으로 향후 행정처분 대상에서 제외

| 참고 : 「사전적정성 검토제」 운영절차 |



※ 신청서 접수에서 법준수방안 협의(위원회 안건상정 준비)까지 2개월 내 처리 원칙

◎ (행태정보 처리) 온라인 행태정보를 처리하는 경우, CPO는 행태정보 처리 방법, 처리환경 등을 면밀히 검토하여 안전하고 적법하게 행태정보를 처리할 수 있도록 관리 필요

- 행태정보 관련 규제 동향을 지속적으로 점검하고, 행태정보 처리에 따른 위험을 정기적으로 식별·평가하여 행태정보를 적법하고 안전하게 처리하기 위한 내부 정책 및 절차 수립·이행

- 행태정보를 직접 처리하는 경우 다른 개인정보와 결합 가능성, 행태정보의 축적에 따른 개인식별 가능성 등을 종합적으로 고려하여 온라인 행태정보가 개인정보에 해당하는지 여부 검토
- 자사의 웹·앱에서 수집도구를 통해 제3자가 수집해가는 행태정보에 현황 관리 및 관련 사항의 투명한 공개 검토 등

◎ (규제 샌드박스 제도 활용) 신기술 환경에서 개인정보를 보호하고 안전하게 활용하기 위해 데이터 이용 현실과 맞지 않는 규제로 인한 어려움이 있는 경우, 개인정보위가 운영 중인 규제 샌드박스 제도를 활용할 수 있음

- (정의) 일정 조건 하에서 혁신적 신기술을 테스트할 수 있게 규제를 유예 또는 면제함으로써 다양한 제품과 서비스가 시장에 출시될 수 있도록 지원하는 제도
- (활용 사례) ① 자율주행·로봇 기업 등이 강화된 안전조치를 준수하면 정보주체의 동의 없이 영상 원본 활용 허용, ② 첨단바이오 분야 국제 공동연구에 필요한 가명정보를 환자 동의 없이도 활용할 수 있도록 허용

CPO 체크리스트

- □ 신기술 도입에 따른 개인정보 위험을 체계적으로 식별·평가 및 조치하기 위한 절차가 마련되어 있는가?
- □ 신기술 도입 시 개인정보 보호 중심설계, 개인정보 영향평가 등의 방안을 통해 신기술 도입에 따른 위험에 대응하고 있는가?
- □ 인공지능 기술의 개발 또는 도입 시 데이터의 수집, 저장·전처리, 학습·모델링·검증, 서비스 제공의 AI 생명주기별로 위험요인을 도출하고 적절한 대책을 마련하고 있는가?

참고자료

- 자동화된 결정에 대한 정보주체의 권리 안내서(개인정보위, 2024.9.)
- 인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서(개인정보위, 2024.7.)
- 스마트도시 개인정보 보호 가이드라인(개인정보위, 2021.12.)
- 생체정보 보호 가이드라인(개인정보위, 2021.9.)

5 개인정보 침해 대응 및 대외협력

5-1 개인정보 침해 민원 대응

• 개인정보 침해 민원은 개인정보처리자의 잠재적 법률 위반 행위 혹은 개인정보 유·노출 사고의 징후일 수 있으므로 CPO는 신속한 대응 체계를 구축 및 운영할 필요가 있음

◆ 개인정보 침해 민원의 유형

○ (내부 접수 민원) 개인정보와 관련된 다양한 민원*이 고객 만족센터, 개인정보보호 담당 부서 등을 통해 접수

* 정보주체 요청사항 처리지연 혹은 미처리, 개인정보 유·노출 사고 의심, 개인정보 보호 의무 이행의 적법성에 대한 이의 제기 등

개인정보 관련 민원 예시

✓ 개인정보 권리 침해 : 개인정보 열람·정정 요청, 수집·이용·제공 동의 철회, 개인정보 처리 정지 요구, 개인정보 이동권 행사, 자동화된 의사 결정에 대한 권리 행사 등이 적시에 처리되지 않음

✓ 개인정보 유·노출 사고 의심 : 로그인 시 정보주체의 서비스가 아닌 타인의 서비스 내역 혹은 개인정보가 송출, 개인정보가 포함된 게시물, 댓글 및 첨부 파일이 서비스내 노출, 검색사이트에 개인정보가 검색됨 등

✓ 적법성 이의 제기 : 개인정보 처리방침내 일부 내용 누락 등

○ (외부 접수 민원) 정보주체는 '개인정보 침해신고센터'를 통해 상담·신고하거나 '개인정보 분쟁조정위원회'에 분쟁 조정을 신청할 수 있음

정보주체의 민원 외부 접수 창구

- **한국인터넷진흥원 개인정보 침해신고센터** : 법 제26조에 근거하여 정보주체가 신고 가능, 제62조에 근거하여 한국인터넷진흥원에서 자료 제출 요구권 및 검사권 위탁 처리, 법률 위반 사항 확인 시 접수일로부터 60일 이내 '행정 지도' 요청, 미시정 시 행정지도 전환 날짜로부터 120일 내 행정 조사 완료
- **개인정보 분쟁조정위원회** : 법 제40조에 근거하여 정보주체는 분쟁 조정을 신청하여 권리를 구제받을 수 있으며 분쟁조정위원회는 사실 조사를 통해 개인정보 권리 침해 중지, 손해배상, 원상회복, 제도 개선 등의 결정을 하며 양 당사자가 수락한 경우(수락 간주 포함) "재판상 화해"의 효력 발생하며 피신청인 불이행 시 강제 집행 가능

민원 대응 절차

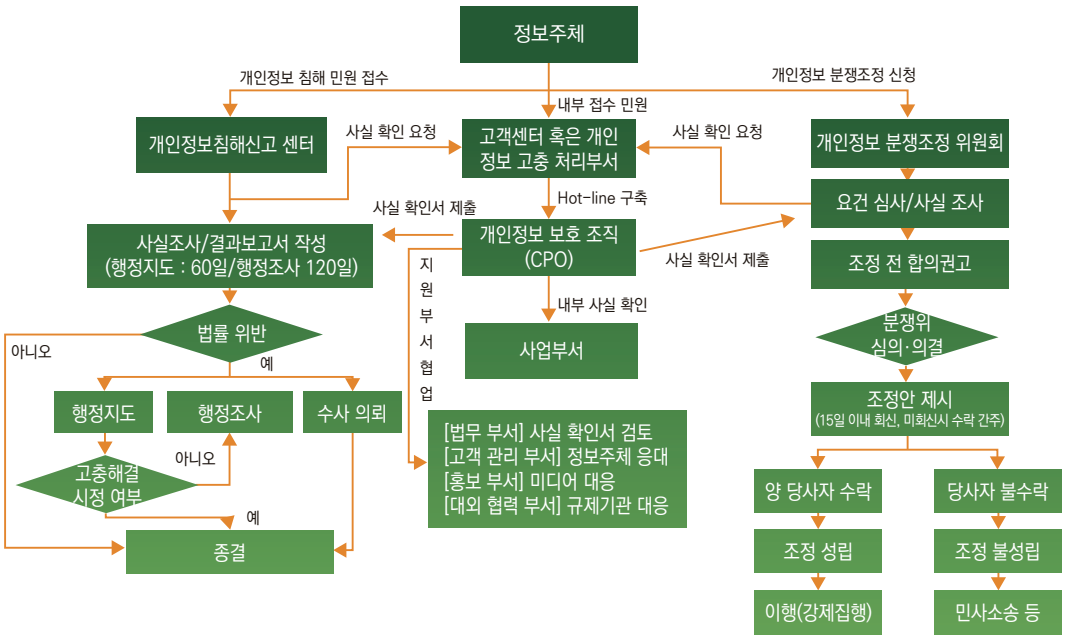
- (신속 전달 체계 구축) 민원 대응을 위해 유관부서와 개인정보 보호 조직 간에 신속한 전달 체계(Hot-line)를 구축하거나 고객센터 내 개인정보 전담 부서를 설치·운영하는 방안 검토
  - 외부 접수 민원의 경우, 요구 기한 내 사실 확인 요청서를 제출해야 하고 유관부서 대상 사실 확인 및 요청서 작성에 시일이 소요되므로 이를 고려하여 신속한 응답 체계 구축 필요
    ※ 민원을 적시에 대응하지 못하는 경우, 정보주체가 개인정보 침해신고센터 등 외부 기관에 민원을 접수할 잠재적 위험 상존

- (사실 확인) 민원 접수 이후, 유관 부서 대상으로 사실 확인 요청
  - (내부 접수 민원) 인터넷 등을 통한 전파 가능성이 있으므로 동일 민원에 대해서는 동일한 답변을 제공하도록 조치
  - (외부 접수 민원) 개인정보 보호 담당 부서에서 사실 확인서를 작성하고 사업 부서 확인 및 법무 부서 검토 후 CPO 승인을 거쳐 제출

| 유관 부서 역할 예시 |

구분	개인정보 보호 조직	유관 부서
사실 확인	· 사실 확인 요청	· IT 조직 등 개인정보처리 부서
사실 확인서 작성	· 초안 작성	· 법무 부서 : 사실 확인서 최종 검토
사실 확인서 제출	· 제출 요청	· 개인정보보호 조직 : 사실 확인서 전달
고객 대상 답변	· 주요쟁점 확인	· 고객만족 부서, 홍보 부서 : 표현의 적절성 등 검토

| 개인정보 민원 대응 체계 예시 |



CPO 체크리스트

- ☐ 고객센터 및 개인정보 보호 조직간 개인정보 침해 민원 전달을 위한 신속 전달 체계가 구축되었는가?
- ☐ 고객 관리 부서 및 법무 부서 등 유관 부서가 개인정보 침해 민원에 따른 잠재적 위험을 이해하고 민원 대응 관련 자신의 역할을 인지하고 있는가?

관련 법령

- 법 제35조(개인정보의 열람)
- 법 제35조의2(개인정보의 전송 요구)
- 법 제36조(개인정보의 정정·삭제)
- 법 제37조(개인정보의 처리 정지 등)
- 법 제37조의2(자동화 결정에 대한 정보주체의 권리)
- 법 제38조(권리행사의 방법 및 절차)
- 법 제39조(손해배상책임)
- 제 39조의2(법정손해배상의 청구)

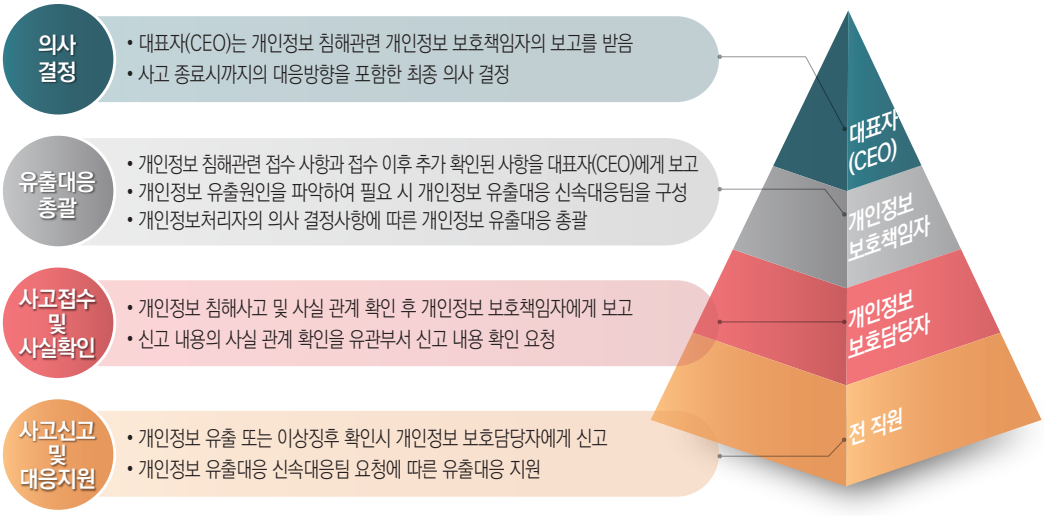
5-2 개인정보 유출 등 사고 대응

• CPO는 개인정보 유출 등의 사고 발생 시 신속한 대응 및 조치를 통한 피해확산 방지, 정보주체에 대한 피해구제를 위해 사고 대응 매뉴얼 개발, 모의훈련 실시, 사고 대응 역량 강화 등 사고 대응을 총괄하여 수행할 필요가 있음

◆ 사고 발생 대응 체계 구축

- (경영진 보고) 개인정보 유출 등 사고 사실을 알게 된 경우, 즉시 회사 내부에 공유하고 경영진에게 보고하는 조직체계 구성
- (사고대응팀 구성) 개인정보 보호 부서 중심으로 유출사고 신속대응팀(이하 '사고대응팀')을 구성하여 피해 최소화 및 확산 방지 조치 필요
  - CPO는 사고 발생 이후부터 해당 시점까지 파악된 현황을 경영진에게 신속하게 보고하고 새로운 상황 발생 시 수시 보고

| 개인정보 유출 등 사고 발생 사실 보고 체계 (예시) |



※ 출처 : 개인정보 유출 등 사고대응 매뉴얼(개인정보위, 2023.9.)

- (평상시 관리 방안) CPO는 개인정보 유출 등 사고 발생 시 신속한 보고 및 대응을 위해 평상시에 대응체계를 구축해야 함
  - 개인정보 유출 사고 대응 계획에 관한 사항을 내부 관리계획에 반영하여 수립·시행
  - 개인정보 유출 사고 대응 매뉴얼 마련
  - 정보보안 부서와 협조하여 정기적으로 유출 사고 발생 대응 훈련을 실시하는 등 개인정보 유출 사고 대응체계 구축

    ※ 유출 사고 대응 계획은 개인정보위 개인정보 유출 등 사고대응 매뉴얼(2023. 9)을 참고하여 개인정보처리자의 조직 특성을 고려하여 수립 가능

◈ 개인정보 유출 등 사고 대응

- (최초 사고 징후 인지) 고객센터에 접수된 민원과 접속 기록 검토 등을 통해 개인정보 유출 사고의 징후 발생 시 CPO에 즉각 보고하고 '사고대응팀' 등 개인정보 유출 등 사고 대응 체계 가동

- (개인정보 유출 등 사고 인지) CPO는 개인정보 보호 부서를 중심으로 정보보안 부서, 법무 부서, 사업 담당 등 유관 부서 협업을 통해 탐지된 징후에 대한 상세 사실관계 확인
  - 사고 여부 및 인지 시점에 대해서는 법무 부서와 정보보안 부서 등 유관 부서와 논의하여 합리적 수준에서 판단

- (긴급 조치) 유관 부서와 협의하여 개인정보 유출 등 사고에 따른 피해 최소화 및 긴급 조치 실시

- (경영진 보고) CPO는 경영진을 대상으로 유출 등 사고 발생 사실 및 긴급 조치 내역을 보고하고 진행 경과를 지속적으로 공유

개인정보 유출 등 사고 발생 원인에 따른 대응 예시

- ✓ 해킹 : 시스템 분리/차단 조치, 로그 등 증거자료 확보, 유출 원인 분석, 이용자 및 개인정보취급자 비밀번호 변경 등
- ✓ 내부자 : 유출 경로 확인, 유출에 활용된 컴퓨터/USB/이메일/출력본 등 확보, 취급자의 접근권한 확인, 비정상 접근 경로 차단 등
- ✓ 이메일 : 발송 이메일 즉시 회수, 수신자에게 오발송 메일 삭제 요청, 대용량 메일 서버 운영자에게 파일 삭제 요청, 파일 전송 시 암호화 등
- ✓ 노출 : (검색엔진)노출된 개인정보 삭제 요청, 로봇 배제 규칙 적용 등, (시스템 오류)소스코드, 서버 설정 등 원인 파악 및 수정 등, (홈페이지 게시)게시글 삭제, 첨부파일에서 개인정보 마스킹 등

정보주체 유출 통지

- (통지문 작성·발송) 정보주체를 대상으로 발송하는 통지문은 인터넷, 언론 취재 등을 통한 전파 가능성이 있으므로 홍보부서와 협의 권고
  - 유출 사고 인지 후 72시간 내에 발송(최종 발송 시점 72시간 이내 처리)
    ※ 통지문 작성 단계 예시: (초안 작성)개인정보 보호 부서 → (초안 검토)개인정보 부서·법무부서→ (톤앤매너 조정)홍보 부서 및 고객 관리 부서 → (최종확인)법무부서 → 발송

- (정보주체 문의 대비) 예상되는 질의응답 사항을 정리하고 고객센터 등 정보주체 접점 상담원 대상으로 교육진행

- (사후 점검) 고객센터를 통한 관련문의 인입추이와 홍보부서 대상으로 관련 언론보도 추이 점검 요청

개인정보 유출신고

- (초안 작성) 개인정보 보호 부서에서 확인된 사실 중심으로 초안 작성 후 유관 부서 검토 및 법무부서의 최종 확인

- (신고 접수) 사고발생시점 72시간 이내에 개인정보 포털 누리집(www.privacy.go.kr)의 '개인정보 유출 신고' 페이지를 통해 신고
  ※ 정상접수 여부 확인을 위해 '유출신고 현황 확인' 메뉴 및 문자 수신여부 확인

| 개인정보 유출 등 사고 발생 대응 단계별 절차(예시) |

단계	주요내용	담당
사고인지 긴급조치	· 개인정보 유출 사고 인지 및 신고 접수 – 사고가 의심되는 경우, 개인정보 보호담당자에게 신고 · 개인정보 보호담당자는 사고 내용 등에 대해 CPO에게 보고 · 개인정보 유출 신고 등 사고 신속 대응팀 구성 · 피해 최소화를 위한 긴급 조치 수행 – 유출된 개인정보 비공개 또는 삭제 조치 – 유출 접속 경로 차단, 취약점 점검 및 보완 등 긴급조치, 재발방지 조치 등	개인정보 유출 부서장, 개인정보 보호담당자, CPO
⬇		
정보주체 유출통지	· 1건이라도 개인정보 유출 시, 정보주체에게 유출사실 통지(72시간 이내) – 유출된 개인정보의 항목, 유출된 시점과 그 경위, 피해 구제절차 등	CPO
⬇		
개인정보 유출신고	· 1천명 이상의 정보주체에 관한 개인정보가 유출 등이 된 경우, 민감정보 또는 고유식별정보가 유출된 경우, 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우	CPO
⬇		
사고분석	· 개인정보 유출 신고 등 사고 신속 대응팀의 조사 및 분석 – 사고 원인 분석, 유출 규모 확인, 사고 원인에 대한 조치 등	개인정보 유출 등 사고 신속대응팀장
⬇		
민원대응	· 민원대응을 위한 별도의 온/오프라인 창구 개설 및 운영 – 피해자 구제방안, 수사 진행상황 등에 대한 답변 방향 결정 및 응대 – 2차 피해 방지를 위한 조치방법 안내 등 고객 불안 해소 조치 및 피해구제 절차 안내	개인정보 유출 부서장 민원부서장
⬇		
유출사고 결과보고	· 개인정보 유출사고 결과보고서 작성 및 보고	개인정보 유출 등 사고 신속대응팀장
⬇		
개선 및 이행점검	· 개인정보 유출사고 사례 전파 교육 및 개선 대책 시행(재발방지)	CPO

자료 제출 요구 및 검사 대응

- (개요) 유출사고 발생 시, 사안의 중대성에 따라 개인정보위 혹은 KISA에서 자료제출 요구 및 검사를 실시할 수 있음(법 제63조)

- (서면 점검) 추가사실 확인을 위한 자료 제출 공문 수령 시 기한내 유관 부서 및 법무 부서 확인 후 서면자료 제출

- (현장 점검 통지 공문 수령) 현장 점검 일정, 확인 및 요청사항 등이 포함된 현장 점검 통지 공문 수령

- (점검 대응 계획 수립 및 내부 공유) 실태점검 일정, 부서별 주요 역할, 점검 대응 매뉴얼 등 실태점검 대응 계획안 수립
  - 점검 대응 계획을 경영진에게(CEO포함) 보고 후 조직 내 협조 요청

- (현장 점검 대응) CPO는 조사관 요청에 따라 인터뷰 진행 및 자료를 제출하도록 지휘하고 조사관이 정리한 사실 확인서에 서명
  - 사실 확인서는 개인정보 유노출 사고 관련 개인정보처리자의 공식 확인 문서이므로 법무부서 등 유관 부서 확인 후 서명 날인

행정 처분 대응

- (사전 통지 대응) 예정 처분에 대한 사전 통지서 내 예정 처분 내용, 처분 원인 사실, 적용 법령 등을 확인
  - 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력, 조사 협조, 자진 시정 등 과태료·과징금 감경 요소 관련 사실을 정리하여 법무 부서 검토를 거쳐 의견서 제출
    ※ 사안에 따라 개인정보위 회의 참석 및 위원 대상 대면 설명 필요성 검토

- (시정조치 통보 대응) 개인정보위 공문 및 과태료·과징금 납부서 수령 후 법무 부서 등 유관 부서 대상 공유 및 대응 방향 논의
  - 행정처분 내 결과 공표 포함시 홍보 부서와 협의하여 미디어 모니터링 및 관련영향 분석·대응

| 개인정보 현장점검 대응 절차(예시) |

구분	설명	CPO 주안점
서면점검	· 개인정보위 자료 제출 요구 공문 수령 · 요구사항에 따라 확인된 사실을 정리하여 기재 · 공문과 함께 개인정보위에 자료 제출	· 확인된 사실을 기반으로 작성하여 유관 부서 확인 및 법무 부서 검토 후 제출
현장점검 준비	· 개인정보위 현장 점검 공문 수령 – 현장 점검 일정, 요구 및 준비 사항 등 포함 · 점검 일정, 부서별 역할 등 점검 대응 계획안을 수립하여 유관 부서 대상 공유 · 조사 진행 회의실 및 요청 자료 등 점검 제반 사항 준비	· 대표자 및 유관 부서 임원이 점검 계획을 명확히 인지할 수 있도록 경영진 대상 전파
현장점검 대응	· 조사관을 통해 점검의 취지 및 일정 등 확인 · 조사관 요청에 따라 개인정보취급자 인터뷰 주선 및 자료 제출 · 조사관이 작성한 사실 확인서 검토 후 CPO 서명 날인	· 주요 인터뷰 내용 및 제출 자료 기록 관리 · 사실확인서는 유관 부서 및 법무 부서 검토를 거쳐 CPO 최종 확인 및 서명 · 점검 결과에 대한 공유
행정처분 대응	· 예정 처분에 대한 사전 통지서내 예정 처분 내용, 처분 원인 사실, 적용 법령 등을 확인 – 필요시 개인정보 보호를 위한 노력 등 과태료·과징금 감경 요소 관련 의견서 제출 · 과태료·과징금 납부서 수령 후 법무 부서 등 유관 부서 대상 공유 및 대응 방향 논의 · 유관 부서 대상 과징금 및 과태료 납부 요청 및 납부 확인	· 행정처분 결과 대표 이사 보고 및 유관 부서 임원 공유 · 처분 결과에 따른 대응 방안 및 영향을 분석하여 최고경영진과 논의 · 유관 부서 임원 대상 기한내 납부 협조 요청

CPO 체크리스트

□ 개인정보 유출 등 사고 대응 체계를 구축하였는가?
- 사고 발생 사실 보고 체계를 구축하였는가?
- 사고 신속 대응팀을 구성 및 운영하는가?
- 사고 대응 매뉴얼을 마련하였는가?

□ 유관 부서 대상으로 개인정보 유출 등 사고 대응 매뉴얼에 따른 모의 훈련을 실시하는가?

□ 개인정보위의 자료 제출 및 현장 점검 대응 체계를 수립하고 이를 유관 부서에 전파하였가?

□ (행정 처분시) 사전통지문 수령 후 처분 대상 사실 및 과태료·과징금 감경 사유 등에 대한 의견서를 유관 부서 협의 후 제출하였는가?

□ (행정 처분시) 과태료·과징금 납부 등 최종 결정 내용을 확인하고 대응 방안을 유관 부서와 논의하였는가?

관련 법령

- 법 제34조(개인정보 유출 등의 통지·신고)
- 신용정보법 제39조의4(개인신용정보 누설통지 등)

참고자료

- 개인정보 유출 등 사고 대응 매뉴얼(개인정보위, 2023.9.)

5-3 조직 내 개인정보 보호 정책 위반 확인 시 대응

• CPO는 조직 내부적으로 개인정보 보호 정책 위반 사항 확인시 개인정보 유출 등의 사고로 확대되지 않도록 즉각적인 개선 조치 및 재발 방지 대책을 마련할 필요가 있음

◆ 위반 확인 및 대응절차

○ (위반 사례 확인) 개인정보처리시스템의 점검, 개인정보 내부 관리계획의 이행 점검, 개인정보 관련 민원 접수 등을 통해 임직원의 내부 개인정보 보호 정책 위반 행위가 확인될 수 있음

- CPO는 사실 확인조사를 위해 관련 자료 제출 및 소명 요청 등의 절차를 수립하고 위반 사례 확인 시 즉각적인 개선 조치 시행
- 형사처벌 대상의 경우 법무부서, 인사부서 논의를 통해 고발 여부 검토

| 규정 위반 사고 예시 |

유형	사례
개인정보 관리 및 보호 활동 소홀	· 경품 발송에 필요한 고객의 개인정보에 암호를 설정하지 않고 PC에 저장하고, 보유기간 도래 후에도 파기하지 않고 보유 · 고객센터로 접수된 고객의 개인정보보호 권리 관련 문의를 적시 처리하지 않고 10일 이상 방치 · 정보처리시스템의 사용자계정·인증수단을 권한 없는 자에게 대여·공유 · 정당한 사유없이 개인정보처리시스템으로부터 고객의 개인정보를 대량으로 다운로드하여 개인 단말기에 저장
개인정보 부정 이용	· 업무상 알게 된 고객의 연락처를 통해 동의 없이 사적 목적으로 연락 · 인사시스템상 개인정보를 취득하여 본인의 소송을 제기하는데 사용
개인정보 무단조회·열람	· 호기심, 공유목적 등 목적 외로 유명인 개인정보를 조회 · 적법 절차를 거치지 않고 고정형 영상정보처리기기 저장된 영상정보 무단 열람·조회

○ (징계 절차 마련) CPO는 인사 부서와 협의하여 개인정보 보호 정책 위반 사례 발생 시 징계 기준 및 절차 마련

- 개인정보의 민감도, 고의성, 과실 정도 등 사안의 경중에 따라 적절한 징계 조치 마련

- (재발 방지 방안의 수립) 유사 사례 재발 방지 및 경각심 제고를 위해 해당 부서 임원 대상으로 재발 방지 방안 수립 요청
  - 또한, 주요 위반 및 징계 사례를 사내 개인정보보호 인식 제고 활동시 전파하여 조직 내 개인정보취급자의 경각심 제고

CPO 체크리스트

- ☐ 개인정보 정책 위반, 개인정보 유출 등 사고 대응 절차가 수립되어 있는가?
- ☐ 조직 내 인사 규정에 개인정보 보호 정책 위반 행위에 대한 징계 절차가 반영되어 있는가?
- ☐ 재발 방지 대책 방안을 수립하였는가?

관련 법령

- 법 제31조 4항, 5항(개인정보 보호책임자의 지정 등)

참고자료

- 개인정보 보호 법규 위반에 대한 징계권고 기준(개인정보위, 2023.10.)

5-4 외부 인증·평가 심사 대응

• CPO는 인증·평가 심사 대응의 총괄 책임자로서, 관련 부서와의 협조체계 구축 후 인증·평가 심사과정에 적극 참여하며, 인증·평가 이후 개선조치 사항에 대해 신속 대응할 필요가 있음

◈ 외부 인증·평가 심사대응 개요

- (현황 관리) 인증·평가 대상이 되는 경우, 심사 대응을 위한 조직 내 대응인력, 예산, 보고체계 등을 마련하고 현황 관리 필요

- (인증·평가 유형) 법 기반의 인증·평가제도는 개인정보 보호수준 평가, 개인정보 영향평가(PIA), 개인정보 처리방침 평가, 정보보호 및 개인정보 보호 관리체계(ISMS-P) 인증 등이 있음
  - 이 외에도 ISO/IEC 27701, CBPR 등 국제 인증·평가 제도 운영 중

개인정보보호 관련 인증·평가의 종류

- 개인정보 보호수준 평가(공공기관에 해당)
  - 근거 : 법 제11조의2, 개인정보 보호수준 평가에 관한 고시
  - 매년 개인정보 보호 정책 · 업무의 수행 및 법에 따른 의무 준수여부 등을 평가하는 제도
- 개인정보 영향평가(공공기관 의무사항에 해당)
  - 근거 : 법 제33조, 개인정보 영향평가에 관한 고시
  - 법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위하여 평가를 진행하는 제도
- 개인정보 처리방침 평가
  - 근거 : 법 제30조의2, 개인정보 처리방침 평가에 관한 고시
  - 개인정보위가 개인정보처리자의 처리방침이 법에 따라 적정하게 작성되었는지, 알기 쉽게 작성되었는지 여부 등을 평가하는 제도
- 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증
  - 근거 : 법 제32조의2, 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시
  - 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 제도

인증·평가 심사 사전준비

- (대응계획) 인증·평가 심사대응 계획을 수립하여 체계적으로 준비

외부 인증·평가 심사 대응 계획 수립 시 고려사항

- ✓ 인증·평가 심사 사전준비부터 본심사, 사후관리 등 전체 진행 일정 확인
- ✓ 인증 종류에 따른 평가기준을 확인하고 관련 부서, 소요자원(인력, 예산) 등 내용 확인
- ✓ 내부 개인정보 보호 조직 인력으로 수행이 어렵다고 판단되는 경우, 외부 전문가 또는 전문 업체를 통해 준비할 수 있도록 검토

- (협력체계 구축) 인증·평가 심사 준비는 개인정보 보호 조직을 중심으로 개인정보 처리 관련 부서와의 협력체계 구축 필요
  - 인증·평가 기준을 분석하여 개인정보보호 부서 및 관련 부서*와의 역할을 분담하고 업무협조를 받도록 해야함

    * 예 : 수탁자와의 계약부서 및 담당자, 개인정보처리시스템 운영부서 및 담당자 등

- (역량 강화) 조직 차원에서 인증·평가 심사 담당 부서와 구성원의 역량 강화를 위한 노력 필요
  - 관련 교육·세미나에 적극 참여하도록 안내하고, 인증·평가 심사에 직·간접적으로 참여할 수 있는 기회 제공

- (증적자료 준비) 인증·평가 기준에 따른 현황 분석 및 점검 수행에 따른 증적자료를 마련하여 인증·평가 심사 준비

  ※ 현황 분석 이후 발견된 미흡사항에 관한 개선조치 등 대책마련 필요

외부 인증·평가 심사 대응 사전준비 수행 사항

- ✓ 인증·평가 기준별 현황 분석 및 점검을 통한 취약점 또는 미흡사항 도출

  ※ 인증·평가 기준별 관련부서와의 협조를 통해 현황분석 수행
- ✓ 확인된 취약점 또는 미흡사항에 대한 개선조치 방안 마련을 통한 개선조치 수행
- ✓ 개선조치 이후 조치된 내용대로 운영되고 있는지에 대한 내부 감사 활동
- ✓ 인증·평가 기준별 요구되는 증적자료 준비

◆ 외부 인증·평가 심사 시 대응

- (적극 지원 및 협조) CPO는 인증·평가 심사 착수 회의에 참여하여 원활한 심사진행이 이루어질 수 있도록 적극적으로 지원 및 협조
- (최종 승인) CPO는 인증·평가 심사 종료 회의에 참여하여 심사에서 지적된 미흡사항을 확인하고 최종 승인을 하도록 함

◆ 외부 인증·평가 심사 사후관리

- (개선조치 계획 수립·이행) CPO는 인증·평가 심사에서 지적된 미흡사항 개선조치를 위해, 이를 수행할 부서와의 협의를 통해 계획 수립 후 이행하도록 안내
- (개선조치 결과 통보) CPO는 미흡사항 개선조치 완료 후, 인증·평가 수행 기관에 개선조치 결과서 통보
- (재발방지) 유사한 미흡사항이 추가발생하지 않도록 관리체계를 수립하고 교육 등을 통해 임직원 인식제고 및 향상을 위해 노력

CPO 체크리스트

- □ 외부 인증·평가 제도에 대해서 CEO, CPO, 관련부서 등이 이해하고 있는가?
- □ 외부 인증·평가 심사를 대응하기 위한 협력체계(조직구성, 전문인력 보유 등) 가 구축되어 있는가?
- □ 외부 인증·평가 심사 완료 후 지적된 미흡사항에 대하여 신속히 개선조치를 수행하고 재발방지를 위한 노력을 하고 있는가?

관련 법령

- 법 제11조의2(개인정보 보호수준 평가)
- 법 제30조의2(개인정보 처리방침의 평가 미 개선권고)
- 법 제32조의2(개인정보 보호 인증)
- 법 제33조(개인정보 영향평가)

참고자료

- 개인정보 영향평가 수행안내서(개인정보위, 2024.4.)
- ISMS-P 인증기준 안내서(과기정통부·개인정보위·KISA, 2023.11.)

5-5 개인정보 자율보호 문화확산

• 개인정보보호 자율규제 및 CPO 협의회 활동을 통해 개인정보보호 정책 변화에 따른 공동대응이 가능함. 또한 조직 내 개인정보 보호 인식제고 활동 효과 극대화를 위해 개인정보 보호의 날 및 개인정보 보호 주간과 연계한 활동 등을 고려하는 것이 필요함

개인정보보호 자율규제

- (개념) 개인정보보호 자율규제란 개인정보보호 문화 확산과 국민의 개인정보 권리 보장을 목적으로 민간 스스로 개인정보 보호를 위한 규약을 만들어 준수하는 자발적 규제 활동

- (효과성) 업계의 산업적 특성에 따른 공통적 개인정보 위험 요인에 대해 동종 업계 개인정보 처리자간 연대를 통한 효과적인 위험관리 고려 가능

업종별 개인정보 위험 예시

✓ (이동통신업) 대리점 및 판매점에 대한 수탁사 개인정보보호 관리·감독 의무 이행

✓ (온라인 플랫폼) 오픈마켓 및 배달 등 온라인 플랫폼을 통해 플랫폼 이용자의 개인정보를 제공받는 중소영세 규모 판매자 혹은 서비스제공자의 개인정보 관리 수준 취약 우려

✓ (의료/사회복지) 의료 보험 혹은 사회복지 지원 관련 정보를 병원, 약국, 복지관 등 중소 규모 의료 기관 및 복지기관의 개인정보보호 관리 수준 취약 우려

- (수행 방식) 업종별 협·단체를 '자율규제단체'로 지정하고 분야별 자율규약을 수립·이행하여 매년 자율점검을 실시하고 개선 지원

  ※ 관련 : 법 제13조 및 개인정보보호 자율규제단체 지정 등에 관한 규정

  - 개인정보위는 자율규제단체 및 회원사 대상으로 인센티브 부여* 등 자율규제 활동을 적극적으로 지원하는 등 민간 주도의 개인정보보호 자율규제 체계 확산 활동 수행 중

    * ① 우수 회원사 대상 자율규제 관련 자료제출 요구 등 1년 면제, ② 우수기관에 대한 과징금·과태료 감경, ③ 개인정보 보호 유공자 포상 등 정보 포상 수여 등

- (고려사항) CPO는 동종업계의 개인정보 위험 공동 대응을 위해 소속 협회 등에 개인정보 자율규제 활동 참여를 제안하고, 해당 업종의 CPO들과의 연대 고려

- 자율규제 활동은 업종별 자율 점검표 혹은 관련 가이드 개발 등 개인정보 처리 현업에 대한 이해와 경험이 기반이 되어야 하므로 개인정보 보호 부서의 직접 참여가 효과적

  ※ 개인정보처리자별 조직 특성 및 업무 분장 현황에 따라 대외협력부서 등의 대관 담당 부서가 참여하고 개인정보 보호 조직 대상 내부적으로 전달 및 의견 수렴하는 방안 또한 고려 가능

CPO 협의회

○ (개요) 개인정보처리자는 CPO를 구성원으로 하여 개인정보의 안전한 처리·보호, 정보의 교류 및 공동 사업 수행을 위하여 CPO 협의회를 구성 · 운영 할 수 있음(법 제31조제7항)

CPO 협의회의 공동 사업(영 제32조의2)

- ✓ 개인정보처리자의 개인정보 보호 강화를 위한 정책의 조사, 연구 및 수립 지원
- ✓ 개인정보 침해사고 분석 및 대책 연구
- ✓ 개인정보 보호책임자 지정 · 운영, 업무 수행 현황 등 실태 파악 및 제도 개선을 위한 연구
- ✓ 개인정보 보호책임자 교육 등 개인정보 보호책임자의 개인정보 보호 역량 및 전문성 향상
- ✓ 개인정보 보호책임자의 업무와 관련된 국내외 주요 동향의 조사, 분석 및 공유

※ 공공시스템운영기관은 공공시스템 운영 수탁사 등과 공공시스템의 안전성 확보 조치 이행상황 점검 및 개선에 관한 사항을 협의하기 위하여 공공시스템운영협의회를 공공시스템별로 설치 · 운영해야 함(영 제30조의2제5항)

○ (고려사항) CPO 협의회는 개인정보보호 관련 주요 동향 파악, CPO 역량 및 전문성 강화 기회 등으로 활용 가능하므로 업종별 개인정보처리 특성 및 조직의 성격 등을 고려하여 협의회 참여 여부를 결정할 수 있음

개인정보 인식제고 활동

○ (인식제고) CPO는 사내 포스터 부착, 퀴즈 이벤트 등 다양한 개인정보 보호 캠페인 기획*을 포함하는 등 인식제고 향상을 위한 노력 필요

* 개인정보 보호 인식주간(매년 9월 마지막 주), 개인정보 보호의 날(매년 9월 30일, 법정기념일) 등과 연계한 추진방안 고려

- 침해사고 사례 전파, 개인정보 보호 수칙 등 개인정보취급자가 쉽게 이해하고 실무에 적용할 수 있는 환경 조성

| 개인정보 보호 인식제고 활동 예시 |

구분	활동
개인정보보호 홍보 콘텐츠 제작 및 게재	· 개인정보보호 수칙 및 포스터 등 홍보 콘텐츠 마련 · 인트라넷/그룹웨어 내 배너 게시, 사내 포스터 부착, 사내 뉴스레터, 기념품 배포 등
임직원 참여 이벤트	· 개인정보 파일 및 문서 파기 캠페인 실시 · 개인정보보호 퀴즈 풀기 및 경품 제공 · 개인정보보호 실천 또는 주의 사례 공모전 · 개인정보보호 표어 또는 경고 문구 공모전 · 개인정보보호 결의 대회 또는 가두 캠페인 실시 · 개인정보보호 외부 전문가 섭외 특강
정보주체 대상 이벤트	· 개인정보보호 실천 또는 주의 사례 공모전 · 개인정보보호 표어 또는 포스터 공모전 · 홈페이지 배너, 뉴스레터, 카드 뉴스, 매장 내 홍보용 포스터 부착 등 · 개인정보보호 온라인 이모티콘 제작 및 배포

ESG와 개인정보 보호

- (개요) 기업의 미래 경쟁력을 결정하는 중요 기준으로 대두되는 ESG(환경·사회·지배구조) 경영에 개인정보 보호가 사회적 책임과 지속 가능성에 직접적인 영향을 미치는 요소인 핵심 ESG 성과 지표로 인식되는 추세 강화

- (고려사항) 조직이 ESG 경영을 위한 진단 항목 설계시, CPO는 개인정보 보호 관련 항목이 반영되도록 건의하여 개인정보 보호 활동이 기업의 지속가능한 경영 가치의 일환으로 전개되도록 추진할 필요

개인정보보호 관련 ESG 진단 항목 예시[8)]

- (개인정보보호를 위한 자율적 노력 및 활동) 개인정보 자기결정권 보장을 위해서 법적 준수사항 외 자율적으로 개인정보 보호를 위해 수행하는 활동 및 노력을 확인
  - 개인정보보호 중심 설계 적용, ISMS-P 인증 획득, 자율규제 활동, 투명성 보고서 발간 등)
- (개인정보 침해 및 구제) 조직이 관리하는 고객, 협력사 등 다양한 이해관계자의 개인정보 침해에 대한 법/규제 요건을 명확하게 인식하고, 개인정보 침해 사건이 발생하였을 경우 이에 대한 구제 활동을 추진하는지 확인
  - 법상 형벌, 행정상 처분(금전적, 비금전적)에 대해 가중치를 달리 적용하는 방식으로 '개인정보 침해 및 구제' 현황을 점검

8) K-ESG 가이드라인 v1.0(관계부처 합동, 2021. 12)

CPO 체크리스트

- □ 동종 업계 공동 대응이 필요한 개인정보 위험을 식별하였는가?
- □ 공동 대응이 필요한 위험 관리를 위해 유관 협회 등을 통해 자율규제 활동 필요성 여부를 검토하였는가?
- □ 개인정보 보호 캠페인 등 인식제고 활동을 하고 있는가?
- □ 개인정보 인식제고 계획 수립 시 개인정보 보호의 날 및 개인정보 보호 주간과의 연계성을 고려하였는가?
- □ ESG 경영 진단 항목에 개인정보 보호 관련 내용을 반영하였는가?

관련 법령

- 법 제13조(자율규제의 촉진 및 지원)
- 법 제31조(개인정보 보호책임자의 지정 등)
- 법 제13조의2(개인정보 보호의 날)
- 법 시행령 제32조의2(개인정보 보호책임자 협의회의 사업 범위 등)
- 개인정보 보호 자율규제단체 지정 등에 관한 규정

참고자료

- 자율규제단체 참여사를 위한 업종별 개인정보 처리 가이드(개인정보위, 2020.12.)

Ⅳ

부록

1 CPO 체크리스트

| 단계별 점검 |

단계	구분	체크리스트	관련 페이지
기획·설계	(4-2) 개인정보 보호 중심 설계(PbD)	· 조직의 특성에 맞는 PbD 정책 및 절차를 마련하였는가? · PbD 절차가 효과적으로 이행될 수 있도록 관련 조직간의 R&R을 명확히 정의하였는가? · 개인정보 영향평가 필요성 검토 절차 및 수행체계(기준, 방법론, 조직, 인력 등)가 마련되어 있는가?	56
	(4-3) 가명정보 관리·감독	· 가명정보 처리 절차, 안전조치 기준, 조직간 R&R 등을 포함하는 가명정보 내부 관리계획을 조직의 특성에 맞게 수립하였는가? · 가명정보 전문가 육성, 교육 등 내부역량 강화를 위한 방안이 마련되어 있는가? · 가명정보를 처리하는 경우 가명정보 내부 관리계획의 이행실태를 정기적으로 점검하고, 문제점 발견 시 개선조치를 이행하고 있는가?	62
	(4-4) 신기술 트렌드 분석 및 대응 방안 마련	· 신기술 도입에 따른 개인정보 위험을 체계적으로 식별·평가 및 조치하기 위한 절차가 마련되어 있는가? · 신기술 도입 시 개인정보 보호 중심설계, 개인정보 영향평가 등의 방안을 통해 신기술 도입에 따른 위험에 대응하고 있는가? · 인공지능 기술의 개발 또는 도입 시 데이터의 수집, 저장·전처리, 학습·모델링·검증, 서비스 제공의 AI 생명주기별로 위험요인을 도출하고 적절한 대책을 마련하고 있는가?	67
개인정보 수집·이용·제공	(3-1) 개인정보 수집 · 이용 및 제공 적법성 관리	· 개인정보 수집·이용 또는 제3자 제공 전에 적법성을 검토하였는가? · 개인정보 수집·이용 또는 제3자 제공 시 동의서 작성에 대한 절차를 마련하였는가? · 개인정보 수집·이용 또는 제3자 제공 시 적법하게 처리되고 있고 동의서 원본을 안전하게 관리를 하고 있는지에 대해 주기적으로 관리·감독하고 있는가?	28
	(3-10) 개인정보의 국외 이전 법적의무 관리	· 개인정보처리자가 제공하는 서비스에 관한 국외 이전(재이전 포함) 흐름을 파악하고 있는가? · 개인정보 국외 이전에 관한 적법한 근거를 분석하고 해당여부를 확인하고 있는가? · 국외 이전에 관해 공개할 내용을 개인정보 처리방침에 공개하고 있는가? · 국외 이전 시 보호조치를 마련하고 있는가? · 중지명령, 지정학적 이슈, 동등성 평가 등 국외 이전 관련 위험에 대응하기 위한 프로세스를 마련하고 있는가?	49
개인정보 보관·파기	(3-5) 개인정보처리 시스템 보호조치 관리	· 정보통신망을 통한 불법적인 접근 및 침해사고 등 안전성 확보를 위한 보호조치를 하고 있는가? · 개인정보처리시스템의 유출 등 침해사고 예방을 위해 취약점 및 법 위반 요소에 대한 주기적 점검을 통해 기술적 보호조치 노력을 하고 있는가? · 개인정보처리시스템에 대한 접속기록 관리 및 주기적 점검을 수행하고 있는가?	39
	(3-6) 개인정보 파기 관리	· 개인정보 파기를 위한 업무 절차를 마련하고 있는가? · 개인정보 파기 대상 현황 파악 및 현행화를 하고 있는가? · 개인정보 파기에 대한 관리·감독을 수행하고 있는가?	41

| 상시 점검 |

구분		체크리스트	관련 페이지
개인정보 취급자 및 위탁 관리	(3-3) 개인정보취급자 관리	· 개인정보취급자 현황을 유형별로 파악하고 관리하고 있는가? · 보안서약서를 제출받고 관리하고 있는가? · 매년 개인정보취급자별로 차등화된 교육 계획을 수립하여 정기적으로 시행하고, 그 결과를 평가하고 있는가? · 개인정보 보호 캠페인 등 인식제고 활동을 하고 있는가?	34
	(3-4) 개인정보 처리 업무 위탁 관리	· 업체 선정 시 개인정보 보호 역량을 갖춘 갖춘 업체 선정 기준을 마련하고 있는가? · 개인정보 처리업무 위탁 계약 시 표준화된 문서를 마련하고 있는가? · 수탁자 개인정보 처리 업무에 대한 관리·감독을 주기적으로 수행하고 있는가? · 계약 종료 시 수탁자의 개인정보 삭제 및 회수에 대한 관리·감독을 수행하고 있는가?	36
이용자 보호 및 피해구제	(3-2) 개인정보 처리방침 관리	· 개인정보 처리방침 수립을 위한 개인정보 처리 현황 분석 등 선행업무를 수행하였는가? · 개인정보 처리방침을 수립하여 공개하고 있는가? · 개인정보 처리방침에 대한 관리·감독을 통해 현행화하고 있는가? · 개인정보 처리방침에 대한 변경관리를 하고 있는가?	32
	(3-7) 정보주체 권리보장	· 조직의 개인정보처리 활동과 관련된 정보주체 권리를 식별하였는가? · 정보주체가 권리 행사가 가능한 정보주체 접점을 식별하였는가? · 정보주체 권리별 처리절차를 표준화하였는가? · 고객센터 등 유관 부서 대상 표준화된 처리절차를 전파하고 교육하였는가? · 정보주체 권리 행사 및 처리 현황을 주기적으로 모니터링하고 있는가?	43
	(5-1) 개인정보 침해 민원 대응	· 고객센터 및 개인정보 보호 조직간 개인정보 침해 민원 전달을 위한 신속 전달 체계 구축되었는가? · 고객 관리 부서 및 법무 부서 등 유관 부서가 개인정보 침해 민원에 따른 잠재적 위험을 이해하고 민원 대응 관련 자신의 역할을 인지하고 있는가?	71
	(5-2) 개인정보 유출 등 사고 대응	· 개인정보 유출 등 사고 대응 체계를 구축하였는가? – 사고 발생 사실 보고 체계를 구축하였는가? – 사고 신속 대응팀을 구성 및 운영하는가? – 사고 대응 매뉴얼을 마련하였는가? · 유관 부서 대상으로 개인정보 유출 등 사고 대응 매뉴얼에 따른 모의 훈련을 실시하는가? · 개인정보위의 자료 제출 및 현장 점검 대응 체계를 수립하고 이를 유관 부서에 전파하였가? · (행정 처분시) 사전통지문 수령 후 처분 대상 사실 및 과태료·과징금 감경 사유 등에 대한 의견서를 유관 부서 협의 후 제출하였는가? · (행정 처분시) 과태료·과징금 납부 등 최종 결정 내용을 확인하고 대응 방안을 유관 부서와 논의하였는가?	74

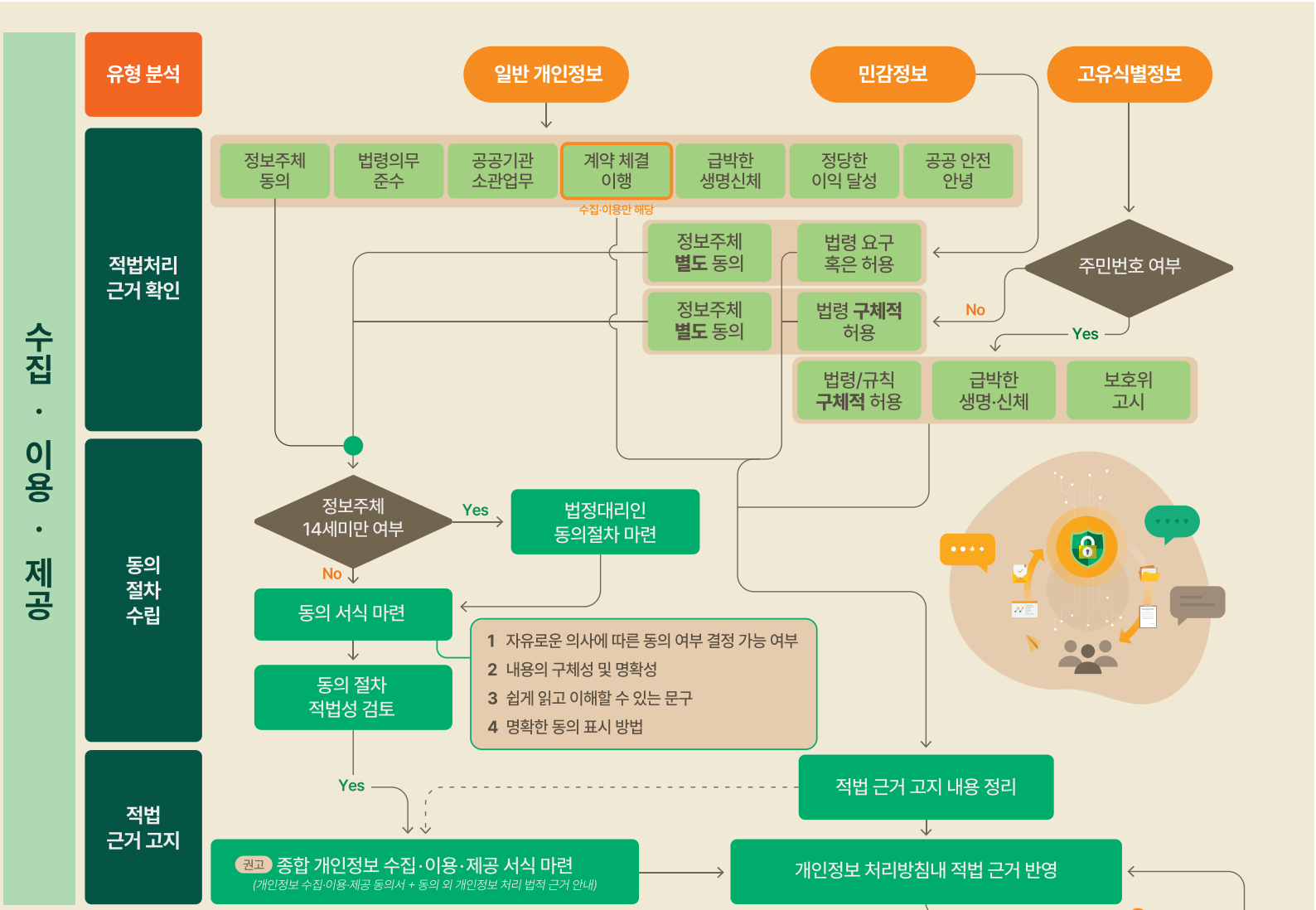
| 주기적 점검 |

구분		체크리스트	관련 페이지
개인정보 처리환경 분석 및 관리	(2-1) 개인정보 생명주기 파악	· 제공 서비스 및 시스템별 처리하는 개인정보 목록을 현행화하고있는가? · 제공 서비스 및 시스템별 처리하는 개인정보 흐름도를 마련하고 있는가? · 주기적인 업데이트를 통해 제공 서비스 및 시스템별 개인정보 흐름도를 최신화하고 있는가?	22
	(2-2) 개인정보처리 시스템 현안파악	· 개인정보처리시스템에 대해 명확히 파악하고, 정기적으로 업데이트 하고 있는가? · 개인정보처리시스템에 대한 접근권한 부여 접근통제, 접속기록 관리 등 안전성 확보조치 구축 여부에 대해 주기적으로 점검 및 개선하고 있는가?	24
	(2-3) 개인정보파일 관리 및 현행화	· 조직 내 처리되는 개인정보 파일의 현황에 대해 주기적으로 확인하고 있는가? · 개인정보 파일에 대한 접근권한 부여 현황, 각 파일에 대한 보유기간 설정, 만료 후 파기절차 구현 여부 등에 대해 주기적으로 점검 및 개선하고 있는가?	26
개인정보 처리 실태 현행화	(3-8) 개인정보 처리 실태 및 관행의 정기적 조사	· 내부 관리계획 이행 실태를 포함한 개인정보 처리 전반의 점검 계획을 체계적으로 수립하고 있는가? · 점검 계획에 따라 점검을 수행하고 그 결과를 경영진에게 보고하고 있는가? · 점검 결과 미흡사항에 대해 재발방지 대책을 포함한 개선조치 계획을 수립·이행하고 있는가?	45
	(3-9) 개인정보파일 관리(공공기관 의무사항)	· 개인정보파일 관리를 위한 업무 절차를 마련하고 있는가? · 개인정보파일 일제정비를 통해 현행화하여 관리하고 있는가? · 개인정보파일 등록 및 공개 의무를 준수하고 있는가?	47
	(5-4) 외부 인증·평가 심사 대응	· 외부 인증·평가 제도에 대해서 CEO, CPO, 관련부서 등이 이해하고 있는가? · 외부 인증·평가 심사를 대응하기 위한 협력체계(조직구성, 전문인력 보유 등) 가 구축되어 있는가? · 외부 인증·평가 심사 완료 후 지적된 미흡사항에 대하여 신속히 개선조치를 수행하고 재발방지를 위한 노력을 하고 있는가?	83

| 성숙도 점검 |

구분		체크리스트	관련 페이지
개인정보 거버넌스	(1-1) 개인정보 거버넌스와 개인정보 조직 체계	· CPO가 CEO 또는 이사회에 직접 보고할 수 있는 체계를 갖추고 있는가? · 핵심 이해관계자 간 책임과 역할을 정의하고 조직 특성을 고려해 적절한 개인정보 보호 조직 체계를 구축하고 있는가? · CPO, CIO, CISO, CFO, 마케팅 및 인사부서 등 개인정보 보호 및 활용 또는 경영 관련 주요 부서 임원이 개인정보 거버넌스 내 자신의 역할과 책임을 명확하게 인식하고 있는가? · 개인정보 보호 조직이 전사적인 개인정보 업무를 수행하는 데 경영진 및 CPO의 지원은 원활하게 제공되고 있는가? · 사내 개인정보보호위원회가 전사적인 개인정보 의제에 관해 내린 결정이 원활히 전파 및 이행되고 있는가? · 개인정보 실무협의체를 통해 개인정보 보호 관련 부서의 협업이 원활하게 이뤄지고 있는가?	13
	(1-2) 개인정보 보호 정책[전략] 수립	· 회사의 개인정보 보호를 위한 정책 및 지침 등이 마련되어 있는가? · 개인정보 보호 정책 등에 대한 이행 및 관리감독이 이루어지고 있는가? · 전사적인 개인정보 위험을 파악하고 관리할 수 있는 절차가 있는가? · 모든 임직원이 개인정보 보호 정책, 지침 및 절차 등에 쉽게 접근 가능한가?	20
위험 관리 및 점검	(4-1) 개인정보 위험관리 체계 구축·점검	· 개인정보 위험을 체계적으로 식별·평가할 수 있도록 조직의 환경에 맞는 위험평가 절차가 마련되어 있는가? · 위험평가 절차에 따라 정기적 및 비정기적으로 개인정보 위험을 평가하고 있는가? · PDCA(Plan-Do-Check-Act) 관점에서 개인정보 위험을 지속적으로 관리하고 있는가?	53
	(5-3) 조직 내 개인정보 보호 정책 위반 확인 시 대응	· 개인정보 정책 위반, 개인정보 유출 등 사고 대응 절차가 수립되어 있는가? · 조직 내 인사 규정에 개인정보 보호 정책 위반 행위에 대한 징계 절차가 반영되어 있는가? · 재발 방지 대책 방안을 수립하였는가?	81
개인정보 자율보호 활동	(5-5) 개인정보 자율보호 문화확산	· 동종 업계 공동 대응이 필요한 개인정보 위험을 식별하였는가? · 공동 대응이 필요한 위험 관리를 위해 유관 협회 등을 통해 자율규제 활동 필요성 여부를 검토하였는가? · 개인정보 보호 캠페인 등 인식제고 활동을 하고 있는가? · 개인정보 인식제고 계획 수립시 개인정보 보호의 날 및 개인정보 보호 주간과의 연계성을 고려하였는가? · ESG 경영 진단 항목에 개인정보 보호 관련 내용을 반영하였는가?	86

2 개인정보 처리 흐름도


수집 · 이용 · 제공
유형 분석
적법처리 근거 확인
동의 절차 수립
적법 근거 고지
일반 개인정보
민감정보
고유식별정보
정보주체 동의
법령의무 준수
공공기관 소관업무
계약 체결 이행
급박한 생명신체
정당한 이익 달성
공공 안전 안녕
수집·이용만 해당
정보주체 별도 동의
법령 요구 혹은 허용
정보주체 별도 동의
법령 구체적 허용
주민번호 여부
No
Yes
법령/규칙 구체적 허용
급박한 생명·신체
보호위 고시
정보주체 14세미만 여부
Yes
No
법정대리인 동의절차 마련
동의 서식 마련
동의 절차 적법성 검토
1 자유로운 의사에 따른 동의 여부 결정 가능 여부
2 내용의 구체성 및 명확성
3 쉽게 읽고 이해할 수 있는 문구
4 명확한 동의 표시 방법
적법 근거 고지 내용 정리
Yes
권고 종합 개인정보 수집·이용·제공 서식 마련
(개인정보 수집·이용·제공 동의서 + 동의 외 개인정보 처리 법적 근거 안내)
개인정보 처리방침내 적법 근거 반영
'파기' 로 이동

추가 이용·제공

'동의 절차 수립'으로 이동

추가 이용 필요

추가 제공 필요

정보주체 별도동의

No

수집 목적 범위와 합리적 관련성 및 안전성 확보 조치 여부

Yes

No

Yes

민감정보·고유식별정보 포함 여부

Yes

No

적법 제공 근거 확인

정보주체 별도 동의	다른 법률 특별 규정	급박한 생명·신체·재산 이익
보호위 심의·의결	조약·국제 협정 이행	범죄 수사 공소 제기·유지
법원 재판 업무 수행	형 및 감호, 보호처분 집행	공공 안전 및 안녕

'동의 절차 수립'으로 이동

추가 이용·제공 판단 기준 개인정보 처리방침 공개

기준에 따른 추가 이용·제공 여부 CPO 점검

동의 없는 추가 이용·제공 가능

추가 이용·제공 지속성 여부

Yes

No

파기

목적 달성 · 보유기간 경과

Yes

다른 개인정보와 분리 보관

Yes

다른 법령상 보존 의무

다른 법령상 보존 의무 기간 경과

No

Yes

개인정보 파기

*
1 당초 수집 목적과 관련성이 있는지 여부
2 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
3 정보주체의 이익을 부당하게 침해하는지 여부
4 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

CPO 핸드북

개 인 정 보 보 호 책 임 자

발행기관 | 개인정보보호위원회·한국개인정보보호책임자협의회(KCPO)

감　　수 | 염흥열 KCPO회장·KCPO 부회장사·감사

㈜LG유플러스 LG전자㈜ SK텔레콤 국립암센터 국민건강보험공단 기아㈜ 넷마블㈜ 메타코리아 삼성서울병원 삼성전자㈜ 삼성화재㈜ ㈜국민은행 ㈜비바리퍼블리카 ㈜우아한형제들 ㈜카카오 ㈜케이티 쿠팡㈜ 한국교통안전공단 한국전력공사 현대자동차㈜ 한국인터넷진흥원 법무법인(유)세종 장준영 변호사

집 필 진 | 강은성 교수 서울여대 김경하 대표 제이앤시큐리티 김도엽 변호사 김·장 법률사무소 옥은택 대표 포유시큐리티 윤수영 대표 에이펙스프라이버시랩 윤호상 변호사 법무법인(유)세종

발 행 일 | 2024년 11월 20일