2025

개인정보보호산업 직무변화 모니터링 보고서

2025. 12.

고용노동부

한국산업인력공단 Human Resources Development Service of Korea

정보보호 인적자원개발위원회 Information Security Industrial Skills Council

2025 개인정보보호산업
직무변화 모니터링 보고서

2025년 12월

연구책임자 : 정보보호ISC 조 연 호 사무총장

참여연구원 : 정보보호ISC 이 보 연 주무팀장

정보보호ISC 이 은 수 주 임

이용자를 위하여

1. 「2025 개인정보보호산업 직무변화 모니터링 보고서」는 고용노동부와 한국산업인력공단의 지원을 받아 정보보호 인적자원개발위원회(ISC)에서 작성하였습니다.

2. 개인정보보호산업 및 직무 현황을 제시할 수 있는 기존 자료를 일부 활용하였으며, 국내 개인정보보호 직무 종사자를 대상으로 인터뷰 및 설문조사를 통해 개인정보보호산업 내 직무 변화에 대한 모니터링을 실시하였습니다.

3. 본 보고서는 개별 사례를 확인·분석하여 계량화된 자료를 통해 파악하기 어려운 직무 현황과 변화를 전반적으로 파악하는 데에 의의가 있습니다.

4. 보고서의 내용을 대외적으로 활용·인용할 시에는 관련 참고문헌 및 데이터 출처는 본문의 해당 자료에도 명시하였으니, 반드시 원 출처를 밝혀주시기 바랍니다.

CONTENTS

2025 개인정보보호산업 직무변화 모니터링 보고서

개요

PART. 01

1 개 요

1. 사업 필요성 및 목적

사업 필요성

- 다양한 환경변화 및 선행요인으로 인해 개인정보보호산업의 직무와 숙련수요가 변화함에 따라 이에 대한 능동적인 대응 필요성 확대
- 효과적이고 활용성 높은 고용·노동 관련 사업 추진을 위해 개인정보보호인력의 실제 직무를 파악하여 개인정보보호 분야 직무맵에 반영하고 국가직무능력표준(NCS) 개발·개선 및 활용·확산 등 유관 사업과의 연계 필요

사업 목적

- 개인정보보호산업에 영향을 미치는 주요 환경변화 요인 및 직무변화 선행요인 파악을 통한 유효한 대응 방안 제시
- 실제 산업현장에서 수행하는 직무의 변화, 세부 과업 및 필요 역량의 변화 등 구체적인 직무·숙련수요 현황 검토를 통한 직무 구분의 적정성 파악 및 직무맵 보완 방향 제시
- 직무변화 모니터링 결과 기반 산업수요에 따른 적절한 인력양성 방안 및 교육·훈련 분야 제시, NCS 개발·개선 직무 발굴 등 인적자원 표준화 및 관련 정책 제언을 위한 기초자료 마련

2. 추진방법

2025년 개인정보보호산업 직무변화 모니터링은 ① 산업 생태계 분석 및 직무 내용 구체화, ② 주요 변화 분석 및 타당성 검증, ③ 결과 분석 및 보고서 작성 등 3단계의 절차를 통해 모니터링을 진행하였다.

추진절차	세부내용	방법
[1단계] 산업 생태계 분석 및 직무 내용 구체화	· 개인정보보호 산업 관련 자료 수집 및 분석을 통한 **문헌조사** 실시	문헌조사
	· 직무맵 기반 직무정의 및 업무범위 등 **직무 내용 구체화**	
	· 영역별 생태계 구성요소 분석 및 개인정보보호산업 **생태계 구조** 도출	전문가 자문
	· **전문가 자문**을 통한 개인정보보호산업 생태계 분석 결과 검토	
↓		
[2단계] 주요 변화 분석 및 타당성 검증	· 직무별 전문가 **심층 인터뷰** 실시	전문가 FGI
	· 직무변화 선행요인, 변화양상, 필요역량 및 수준 등 **세부 변화 내용 분석**	
	· **산업 종사자 대상 설문조사**를 통한 분석 내용의 적정성 및 타당성 검증	설문조사
	· **전문가 자문**을 통한 분석 내용 및 직무맵에 대한 의견 수렴	전문가 회의
↓		
[3단계] 결과 분석 및 보고서 작성	· 모니터링 결과에 따른 **직무변화 선행요인 및 직무변화 양상** 분석	보고서 발간
	· 개인정보보호산업 직무변화 모니터링 **결과 및 시사점** 도출	
	· 개인정보보호산업 직무분석을 통한 **직무맵 보완 및 현행화**	
	· 선제적인 인력양성이 필요한 **신규 교육·훈련 분야 제시**	
	· 차년도 정보보호 ISC 직무변화 **모니터링 수행 방향 제언**	

2025 개인정보보호산업 직무변화 모니터링 보고서

직무변화 모니터링 과정

PART. 02

2 직무변화 모니터링 과정

1. 문헌조사

개인정보보호 분야의 국가직무능력표준(NCS), 직무맵, 산업계 선행연구보고서 등 인적자원 개발 및 분석을 위해 활용되고 있는 보고서를 참고하여, 직무변화 모니터링 사업 수행에 활용할 자료를 정리하였다.

용어정의

- 「개인정보 보호법」 제2조(정의)에서는 다음과 같이 주요 용어를 정의하고 있다.

1. "**개인정보**"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
   가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
   나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
   다. 가목 또는 나목을 제 1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
2. "**처리**"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. "**정보주체**"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. "**개인정보파일**"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. "**개인정보처리자**"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
6. "**공공기관**"이란 다음 각 목의 기관을 말한다.
   가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 소속 기관, 지방자치단체
   나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
7. "**고정형 영상정보처리기기**"란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

7의2. "**이동형 영상정보처리기기**"란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

8. "**과학적 연구**"란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.

* 출처: 국가법령정보센터(www.law.go.kr)

‘개인정보보호 및 활용조사’에서는 다음과 같이 주요 용어를 정의하고 있다.

용어	정의
가명처리	· 가명처리: 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것 · 가명정보: 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보 · 가명정보 처리: 가명정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말함
개인정보	· 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함) * 예시: 성명, 주민등록번호, 전화번호, 주소, 가명정보, 이메일, 사진, CCTV 개인영상정보, 학력, 근무경력 등
개인정보 수집동의	· 사업자나 공공기관이 개인정보 수집, 이용하고자 할 때는 해당 고객, 임·직원 또는 민원인 등에게 ① 수집 이용 목적, ② 수집 항목, ③ 보유 및 이용기간, ④ 동의 거부권 및 거부에 따르는 불이익을 알리고 동의를 받아야 함
개인정보 처리방침	· 처리하는 개인정보의 항목, 개인정보의 처리 목적, 처리 및 보유 기간, 파기절차 및 방법 · 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항 · 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서에 관한 사항 · 개인정보의 안전성 확보조치에 관한 사항 등 ※ 아래 항목은 해당되는 경우에만 정함 · 개인정보의 제3자 제공에 관한 사항 · 민감정보의 공개 가능성 및 비공개를 선택하는 방법 · 개인정보처리의 위탁에 관한 사항 · 가명정보의 처리 등에 관한 사항 · 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
개인정보 보호책임자 (CPO, Chief Privacy Officer)	· 「개인정보 보호법 시행령」 제32조에 따라 공공기관의 개인정보처리자는 다음 각 구분에 따른 사람(공무원 등)을 책임자로 지정하여야 함 ① 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관 ② 정무직공무원을 장(長)으로 하는 국가기관 ③ 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관 ④ 기타 국가기관(소속 기관을 포함) ⑤ 시·도 및 시·도 교육청 ⑥ 시·군 및 자치구 ⑦ 학교 ⑧ 기타 공공기관

용어	정의
마이데이터	· 마이데이터란 정보주체가 본인의 데이터에 대한 권리를 가지고 자신의 통제권 하에 개인정보를 관리하고 처리하는 제도('23.3월 개인정보 보호법 개정) · 개인정보 유출·피해 방지 등을 넘어 국민의 개인정보 자기결정권을 보장*하는 적극적 프라이버시 권리 * 정보주체가 개인정보를 보유한 기업·기관에게 본인/제3자 전송요구권을 행사하여 데이터를 이동시켜 서비스에 활용할 수 있도록 하는 자기결정권 · 마이데이터 서비스 유형 ① (맞춤형 서비스) 내 정보를 분석하여, 개인 맞춤형 상품 추천 및 서비스를 제공 ② (컨설팅) 진학상담, 재테크 설계 등 전문 컨설팅을 받을 수 있는 서비스 ③ (전자증명서 발급) 종이 서류 없이 개인의 증명서를 전자적으로 이동해 주는 서비스 ④ (통합조회) 나의 개인정보를 한 곳에 모아 금융거래, 항공내역 등을 통합조회하는 서비스 ⑤ (개인정보저장소) 분야에 관계없이 다양한 내 정보를 한곳에 모아서 보관해 주는 서비스 ⑥ (경제적 보상) 내 개인정보를 활용토록 하고 그 대가로 포인트나 쿠폰 등 리워드를 주는 서비스
위수탁	· 개인정보처리자(위탁자)가 특정 업무 수행을 목적으로 업무 수행의 전부 또는 일부를 제3자(수탁자)에게 위탁하여 수행하는 과정에서 개인정보가 처리되는 경우
정보주체	· 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람(해당 개인정보의 주인)
제3자 제공	· 사업자(공공기관)가 자신의 업무나 이익을 위해 제3자(다른 사업자, 기관, 단체, 개인)로부터 개인정보를 제공받는 경우

* 출처: 개인정보보호위원회, 「2024 개인정보보호 및 활용조사」

직무구분

- 국가직무능력표준(NCS)에서는 개인정보보호 분야 직무를 다음과 같이 구분하고 있다.

* **국가직무능력표준(NCS, National Competency Standards):** 산업 현장의 직무를 수행하기 위해 필요한 능력(지식, 기술, 태도)을 국가적 차원에서 표준화 한 것으로 능력단위 또는 능력단위의 집합

➲ **(대분류)** 20.정보통신 〉 **(중분류)** 01.정보기술 〉 **(소분류)** 11.개인정보보호

직무명	직무정의	능력단위
01. 개인정보보호 관리운영	개인정보보호관리운영은 개인정보보호 관련 법령 및 정책에 따라 개인정보를 생명주기별로 안전하게 보호하고 체계적으로 관리·운영하는 일이다.	개인정보보호 법령·정책 분석
		개인정보보호 기획
		개인정보보호 위험관리
		개인정보보호 운영
		개인정보 생명주기 관리
		개인정보 수탁자 관리
02. 개인정보 가명·익명처리	개인정보 가명·익명처리란 개인정보를 법령 등에 따라 정보주체의 동의 없이 안전하게 활용하기 위하여 적정한 수준으로 가명·익명처리를 수행하고 사후관리를 하는 일이다.	가명·익명 법제도분석
		가명·익명처리 기획
		가명·익명 위험관리
		가명·익명처리
		가명정보 결합·반출
		가명·익명처리 적정성 검토
		가명·익명 사후관리
03. 개인정보 인증·평가	개인정보 인증·평가는 개인정보처리자를 대상으로 개인정보보호 기준 준수 여부를 심사하고 평가하는 업무를 수행하는 일이다.	개인정보 인증심사 준비
		개인정보 인증심사 착수
		개인정보 관리체계 진단
		개인정보 안전조치 진단
		개인정보 처리단계별 보호조치 진단
		개인정보 인증심사 종료
		개인정보 인증심사 사후관리

○ 직무맵에서는 개인정보보호 분야 직무를 다음과 같이 구분하고 있다.

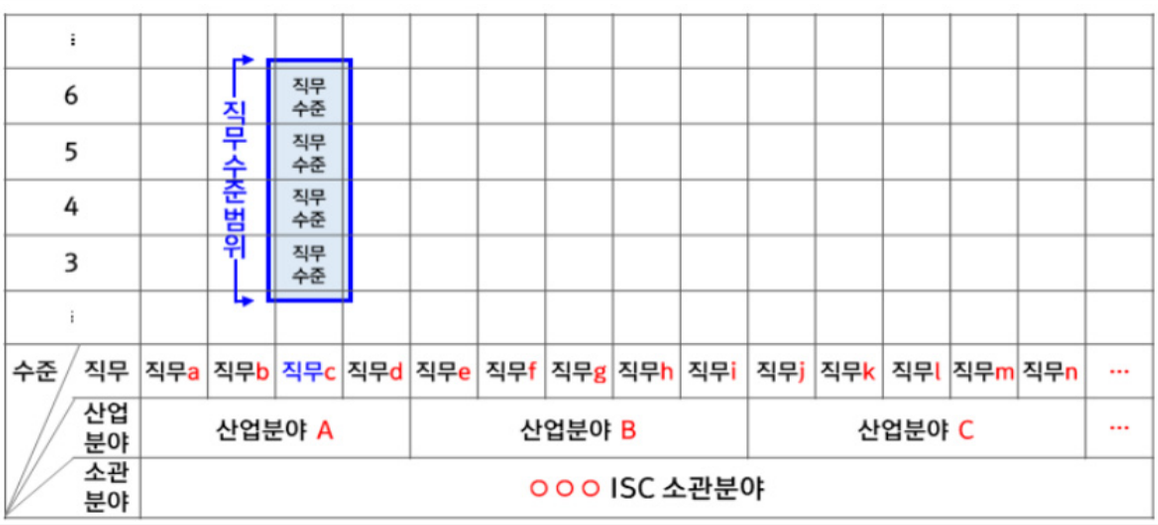
* **직무맵**: 현장에서 통용되는 직무를 도출하여 표준화하고 수준범위를 설정한 것

수준 \ 직무	개인정보 가명·익명처리	개인정보보호 관리	개인정보보호 운영	개인정보보호 컨설팅	개인정보 이동활용관리	개인정보 인증·평가
8						
7						
6						
5						
4						
3						
2						
1						
Sector	개인정보보호					
참여주체	정보보호 ISC					
개발연도	'22년 개발					

참고

[직무맵] 구성

- 가로축은 직무의 유형(type), 세로축은 직무의 수준(level)으로 구성



* 출처: 한국산업인력공단, 산업별역량체계(SQF) 개발 매뉴얼

직무명	정 의(안)	키워드
개인정보 가명·익명처리	개인정보 가명·익명처리란 개인정보를 법령 등에 따라 정보주체의 동의 없이 안전하게 활용하기 위하여 적정한 수준으로 가명·익명처리를 수행하고 사후관리를 하는 일이다.	가명·익명 법제도 분석 / 가명·익명처리 기획 / 가명·익명 위험관리 / 가명·익명처리 / 가명정보 결합·반출 / 가명·익명처리 적정성 검토 / 가명·익명 사후관리
개인정보보호 관리	개인정보보호 관리는 개인정보 법령 및 정책을 기반으로 조직의 개인정보 보호계획 수립, 위험관리, 기술적/관리적 보호조치를 통해 개인정보 관리를 수행하는 일이다.	개인정보보호 법령·정책 분석 / 개인정보보호 기획 / 개인정보보호 위험관리 / 개인정보 분쟁조정 / 개인정보 생명주기 관리 / 개인정보 기술적 보호조치 / 개인정보 관리적 보호조치
개인정보보호 운영	개인정보보호 운영은 내부 개인정보보호 관리계획에 따라 처리시스템을 운영하고 침해/유출 사고에 대응하며 개인정보취급 업무를 수행하는 일이다.	개인정보보호 내부 관리 계획 / 개인정보 처리시스템 운영 / 수탁사 관리·감독 / 개인정보 암호화 / 개인정보 침해·유출 사고 대응 / 정보주체 권리보장
개인정보보호 컨설팅	개인정보보호 컨설팅은 개인정보보호 환경 분석 및 위험평가를 통해 보안모델을 설계하고 개인정보보호시스템 품질을 관리하여 개인정보 안전성 확보를 지원하는 일이다.	개인정보보호 환경 분석 / 개인정보보호 수준진단 계획 수립 / 개인정보보호 위험평가 / 개인정보보호 보안모델 설계 / 개인정보보호 이행계획 수립 / 개인정보보호시스템 품질 관리
개인정보 이동활용관리	개인정보 이동활용관리는 개인정보의 안전한 이동과 활용을 위해 서비스를 기획하여 운영하고 이용자를 교육하는 일이다.	개인정보 활용 서비스 기획 / 마이데이터 서비스 운영 / 데이터 안심구역 운영 / 개인정보 보호·활용 교육 / 개인정보 활용 서비스 품질관리
개인정보 인증·평가	개인정보 인증·평가는 개인정보처리자를 대상으로 개인정보보호 기준 준수 여부를 심사하고 평가하는 업무를 수행하는 일이다.	개인정보 인증심사 준비 / 개인정보 인증심사 착수 / 개인정보 관리체계 진단 / 개인정보 안전초지 진단 / 개인정보 처리단계별 보호조치 진단 / 개인정보 처리시스템 기술적 보호조치 점검 / 인증평가 보고서 작성·배포

기타

유관 부처 및 기관에서 정기적으로 발간·운영하고 있는 개인정보보호 관련 보고서와 누리집을 참고하여 산업 생태계 분석, 심층 인터뷰 및 산업현장 검증 대상자 선정 등에 활용하였다.

구분		명칭	비고
보고서	개인정보보호위원회	· 개인정보보호 및 활용조사 보고서	매년 3월경 발행
		· 개인정보보호 연차보고서	매년 하반기 발행
		· 개인정보 기술 백서	-
	한국인터넷진흥원	· 개인정보 월간동향 보고서	매달 발행
		· 개인정보 이슈 심층 분석 보고서	상시 발행
		· 개인정보 기술포럼 동향보고서	-
누리집		· 개인정보보호위원회 (www.pipc.go.kr)	-
		· 한국CPO포럼 (www.cpoforum.or.kr)	-
		· 한국개인정보보호책임자협의회 (kcpo.or.kr)	-
		· 개인정보 포털 (www.privacy.go.kr)	-
		· 가명정보 지원 플랫폼 (dataprivacy.go.kr)	가명정보 전문가풀, 결합전문기관
		· 차세대 ISMS-P 디지털 플랫폼 (isms-p.or.kr)	-
		· 데이터안심구역 (dsz.kdata.or.kr)	데이터안심구역 지정기관
		· 마이데이터 종합포털 (www.mydatacenter.or.kr)	-
		· 범정부 마이데이터 (www.onmydata.go.kr)	-
		· 공공 마이데이터 업무포털 (adm.mydata.go.kr)	-

○ '개인정보보호 및 활용조사'에서는 다음과 같이 개인정보 활용주체를 구분하고 있다.

구분	세부분류			
개인정보 처리자	공공기관	· 행정기관(중앙행정기관, 광역지자체, 기초지자체, 교육청, 지정공공기관, 지방공기업)		
		· 교육기관(초·중등교육기관, 고등교육기관)		
		· 공공병원		
	민간기업	· 제조	· 전기/가스/수도	· 건설
		· 유통/물류/도소매	· 숙박/음식점	· 정보통신
		· 금융/보험	· 부동산	· 교육서비스
		· 보건/복지 서비스	· 협회/단체	· 기타
정보주체	일반국민	· 일반국민		
	청소년	· 청소년		

* 출처: 개인정보보호위원회, 「2024 개인정보보호 및 활용조사」

○ 개인정보보호 국제표준화를 주도적으로 추진하는 표준화 그룹에서는 다음과 같이 프라이버시 프레임워크, 비식별 처리 등 개인정보 보호 및 활용에 대한 글로벌 표준을 제공하고 있다.

표준	명칭	내용
ISO/IEC 20889	데이터 비식별처리 용어 정의 및 기술 분류	직접, 간접, 준식별자 등에 대한 개인정보의 기술적 용어 정의 및 암호화 도구 등 정형 데이터를 대상으로 한 비식별 처리 기술에 대해 8가지 카테고리에서 총 22가지의 세부기술로 분류하여 제시
ISO/IEC 27701	개인정보관리 요구사항 및 가이드라인	조직 내에서 개인정보관리를 위한 개인정보관리체계(PIMS) 수립, 구현, 유지 및 지속적인 개선을 위한 지침 제공
ISO/IEC 29003	온라인 신원증명	온라인에서 사용자에 대한 신원을 증명하는 가이드라인을 제공하고, 신원 확인을 위한 등급, 그리고 이 등급을 만족하기 위한 요구사항을 제시
ISO/IEC 29100	프라이버시 프레임워크	프라이버시 관련 용어, 개인정보처리에 있어서 주요 주체의 역할, 보호 요구사항, 프라이버시 보호 원칙 등을 포함한 프라이버시 프레임워크 제시
ISO/IEC 29184	온라인 고지 및 동의	정보주체로부터 개인정보를 수집하고 처리하기 위한 동의를 요구하는 온라인 프라이버시 고지와 문서의 내용과 구조를 규정
ISO/IEC 2nd CD 27555	개인정보 삭제 가이드라인	삭제, 삭제기간 등에 대한 용어, 필요한 문서화, 역할, 책임성 등을 정의하고 있으며 개인정보 파기 절차 수립을 위한 프레임워크를 제시
ISO/IEC 1st WD 27559	데이터 비식별화 프레임워크	비식별화된 데이터의 수명 주기와 관련된 위협과 재식별 위험을 찾고 완화하기 위한 프레임워크 제공
ISO/IEC 21st WD 27560	동의 레코드 정보 구조	데이터 주체의 데이터 처리 동의를 기록하기 위해 상호운용가능하고 개방적이며 확장 가능한 정보 구조를 정의
ITU-T X.1148	통신서비스 제공자들을 위한 비식별처리 프레임워크	특정 개인을 식별할 수 없도록 데이터의 생명주기 상태(수집→저장→이용→배포·파기)에 따라 비식별 처리지점과 그 특징 및 보안 고려 사항을 정의
Study Period	인공지능의 프라이버시 영향	인공지능 프라이버시 영향을 평가하기 위한 국제표준으로 사전 연구 활동이 진행중

2. 산업체 의견수렴 및 검증

개인정보보호 분야 직무맵을 기반으로 총 6개 직무별 심층 인터뷰와 산업현장 검증을 진행하였다.

전문가 심층 인터뷰

직무별로 다양한 의견수렴을 통해 전반적인 변화양상을 파악하고자, 문헌조사와 개인정보보호산업 생태계 분석 내용을 기반으로 기업 형태와 규모를 고려하여 인터뷰 대상 기업 및 개인정보보호 담당자를 선정하였다.

- 기　간: 2025년 9월 ~ 11월
- 대상자: 총 15개 개인정보보호 유관 기업 및 일반기업의 개인정보보호 직무 담당자

연번	직무	구분		기업구분	기업규모	업종
1	개인정보 가명·익명처리	1차	가명정보 전문가	대기업계열사	1,000명 이상	반도체 제조용 기계 제조업
2				대기업 계열사	1,000명 이상	통신 공사업
3				공공	1,000명 이상	종합 병원
4		2차	데이터 결합전문기관	중견	1,000명 이상	컴퓨터 프로그래밍 서비스업
5				대기업	1,000명 이상	지주회사
6	개인정보보호 관리	1차	개인정보 보호책임자 (CPO)	중소	100명 대	그 외 기타 금융 지원 서비스업
7				스타트업	100명 대	시스템·응용 소프트웨어 개발 및 공급업
8	개인정보보호 운영	1차	개인정보보호 담당자	중견	1,000명 이상	시스템·응용 소프트웨어 개발 및 공급업
9				대기업 계열사	1,000명 이상	자동차 임대업
10	개인정보보호 컨설팅	1차	개인정보보호 컨설턴트	중소	400명 대	시스템·응용 소프트웨어 개발 및 공급업
11				중소	100명 이하	그 외 기타 정보 서비스업
12		2차		외국계	100명 이하	컨설팅·연구·조사
13	개인정보 이동활용관리	1차	마이데이터 사업자	대기업 계열사	500명 대	시스템·응용 소프트웨어 개발 및 공급업
14		2차	데이터안심구역 지정기관	공공	1,000명 이상	송전 및 배전업
15	개인정보 인증·평가	1차	ISMS-P 인증심사원	중소	100명 이하	시스템·응용 소프트웨어 개발 및 공급업

○ 주요 질의 내용: 산업 환경 변화, 직무 구분 변화, 직무 역량 변화, 인력 수요 등

연번	구분	질문
1	산업 환경 변화	· 개인정보보호산업은 최근 5년 전과 비교해서 어떻게 달라지고 있다고 생각하십니까?
2		· 해당 산업의 환경 변화를 초래하는 요인은 무엇이라고 생각하십니까?
3	직무 구분 변화	· 현재 개인정보보호산업에서의 신규생성, 소멸/축소, 통합/분할되고 있는 직무는 무엇이라고 생각하십니까?
4		· 해당 직무구분 변화에 가장 큰 영향을 미치는 요인은 무엇이라고 생각하십니까?
5		· 기개발된 국가직무능력표준(NCS)과 직무맵은 현재 산업현장의 직무 구분과 얼마나 적합하다고 생각하십니까?
6		· 현재 소속된 기업/기관에서 운영되고 있는 개인정보보호 관련 부서/직무는 무엇입니까?
7	직무 역량 변화	· 담당하고 계시는 개인정보보호 분야 직무의 주요 업무는 무엇입니까?
8		· 담당하고 계시는 개인정보보호 분야 직무 담당자가 되기 위해 필요한 기술(사용 툴, 지식 등)은 무엇이라고 생각하십니까?
9		· 담당하고 계시는 개인정보보호 분야 직무 담당자가 되기 위해 필요한 자격(학위, 자격증, 교육, 경력 등)은 무엇이라고 생각하십니까?
10		· 담당하고 계시는 개인정보보호 분야 직무 수행 능력 향상을 위해 필요한 역량(소프트 스킬, 태도 등)은 무엇이라고 생각하십니까?
11		· 말씀해주신 필요 기술, 자격, 역량 등은 최근 5년 전과 비교해서 어떻게 달라지고 있다고 생각하십니까?
12		· 해당 변화에 가장 큰 영향을 미치는 요인은 무엇이라고 생각하십니까?
13		· 사내에서는 해당 직무변화에 어떻게 대응하고 계십니까?
14		· 향후 개인정보보호산업의 직무가 어떻게 변화(예상변화, 변화속도 등) 될 것이라고 예상하십니까?
15	인력 양성	· 개인정보보호산업에서 가장 인력수요가 높은 직무는 무엇이라고 생각하십니까?
16		· 개인정보보호 직무 담당자가 되기 위해 가장 필요한 교육은 무엇이라고 생각하십니까?
17	기타	· 개인정보보호산업 및 직무변화와 관련하여 추가 의견이 있으시다면 말씀해주십시오.

산업현장 검증

심층 인터뷰 내용의 적정성 검증 및 추가 의견 도출을 위해, 개인정보보호 솔루션 운영 기업 및 일반기업의 개인정보보호 업무를 수행하고 있는 직무 담당자를 대상으로 직무변화에 대한 산업현장 검증을 진행하였다.

- 기　간: 2025년 11월 ~ 12월
- 방　법: 서면 설문조사
- 대상자: 총 30개 개인정보보호 유관 및 일반기업의 개인정보보호 직무 담당자

연번	기업구분	기업규모	업종	비고
1	대기업	100명 대	지주회사	개인정보보호 제품/서비스 운영
2		200명 대	전자상거래 소매업	개인정보보호 담당자
3		500명 대	시스템·응용 소프트웨어 개발 및 공급업	개인정보보호 담당자
4		600명 대	호스팅 및 관련 서비스업	개인정보보호 제품/서비스 운영
5		1,000명 이상	그 외 기타 전자부품 제조업	개인정보보호 담당자
6		1,000명 이상	기타 이차전지 제조업	개인정보보호 담당자
7		1,000명 이상	백화점	개인정보보호 담당자
8		1,000명 이상	보안시스템 서비스업	개인정보보호 제품/서비스 운영
9		1,000명 이상	호텔업	개인정보보호 담당자
10	중견기업	200명 대	시스템·응용 소프트웨어 개발 및 공급업	개인정보보호 제품/서비스 운영
11		1,000명 이상	그 외 기타 정보 서비스업	개인정보보호 담당자
12		1,000명 이상	모바일 게임 소프트웨어 개발 및 공급업	개인정보보호 제품/서비스 운영
13		1,000명 이상	물질성분 검사 및 분석업	개인정보보호 담당자
14		1,000명 이상	시스템·응용 소프트웨어 개발 및 공급업	개인정보보호 제품/서비스 운영
15	중소기업	100명 이하	그 외 기타 정보 서비스업	개인정보보호 담당자
16		100명 이하	기타 육상 운송지원 서비스업	개인정보보호 담당자
17		100명 이하	비주거용 건물 임대업	개인정보보호 제품/서비스 운영
18		100명 이하	시스템·응용 소프트웨어 개발 및 공급업	개인정보보호 제품/서비스 운영
19		100명 이하	시스템·응용 소프트웨어 개발 및 공급업	개인정보보호 제품/서비스 운영
20		100명 이하	시스템·응용 소프트웨어 개발 및 공급업	개인정보보호 제품/서비스 운영
21		100명 이하	시스템·응용 소프트웨어 개발 및 공급업	개인정보보호 담당자
22		300명 대	시스템·응용 소프트웨어 개발 및 공급업	개인정보보호 제품/서비스 운영
23		400명 대	유선 통신장비 제조업	개인정보보호 담당자
24	공공	100명 대	기타 교육지원 서비스업	개인정보보호 담당자
25		200명 대	경영 컨설팅업	개인정보보호 담당자
26		200명 대	교육관련 자문 및 평가업	개인정보보호 담당자
27		200명 대	항구 및 기타 해상 터미널 운영업	개인정보보호 담당자
28		600명 대	기금 운영업	개인정보보호 담당자
29		700명 대	보건 및 복지 행정	개인정보보호 담당자
30		1,000명 이상	국내은행	개인정보보호 담당자

○ 주요 질의 내용: 일반현황, 직무변화 선행요인, 직무별 세부내용 등

연번	구분	질문
1	일반현황	· 기업명, 대표자 성명, 소재지, 기업형태, 전체 종사자수, 개인정보보호 제품/서비스 운영 여부, 사내 개인정보보보호 담당 부서 등
2	직무변화 선행요인	· 최근 개인정보보호산업의 직무나 일하는 과정의 변화를 초래하는 요인이 무엇이라고 생각하십니까? (복수선택 가능)
3		· 해당 응답을 선택한 구체적인 이유는 무엇입니까?
4	직무별 세부내용	· 개인정보보호산업 직무 구분이 얼마나 적절하다고 생각하십니까?
5		· 직무가 적절하지 않다고 생각하는 이유는 무엇입니까?
6		· 현재 산업 내 성숙도를 선택하여 주십시오.
7		· 전체 인력의 수준을 범위로 선택하여 주십시오.
8		· 지난 5년간의 전체적인 직무 변화도를 선택하여 주십시오.
9		· 변화 요인은 무엇이라고 생각하십니까? (복수선택 가능)
10		· 기타 변화 요인이 있다면 무엇입니까? (해당 직무에만 응답)
11		· 향후 5년 이내 인력수요 전망을 선택하여 주십시오.
12		· 현재 구분된 직무 외에 신생직무, 소멸직무, 대체직무가 있다면 관련하여 자유롭게 작성하여 주시기 바랍니다.
13	기타	· 개인정보보호 분야의 직무 및 직무변화와 관련하여 기타의견이 있으면 자유롭게 작성하여 주시기 바랍니다.

2025 개인정보보호산업 직무변화 모니터링 보고서

개인정보보호산업 생태계 분석

PART. 03

3 개인정보보호산업 생태계 분석

* ‘Ⅲ. 개인정보보호산업 생태계 분석’은 한국개인정보보호책임자협의회의 자문을 받아 작성되었습니다.

1. 개인정보보호산업의 개념

개인정보보호산업에 대한 법적·정책적·학술적 개념은 아직 본격적으로 확립되지 않았으며, 국내 개인정보보호산업에 대한 체계적인 분석과 검토 또한 거의 이루어진 바 없다. 반면, 개인정보보호와 밀접한 관련이 있는 정보보호산업에 대해서는 개념 정의 및 산업 활성화 등의 법제도적 기반 마련과 산업 생태계 분석 등 다양한 측면에서 연구와 분석이 다수 이루어진 바 있으며 개인정보보호 관련 산업이 정보보호산업의 하위 분류로써 일부 분석된 사례도 존재한다. 이에, 개인정보보호산업의 개념 도출을 위해 우선 정보보호산업에 대한 개념을 살펴보고자 한다.

「정보보호산업의 진흥에 관한 법률」 제2조에서는 정보보호산업을 ‘정보보호를 위한 기술 및 정보보호기술이 적용된 제품을 개발·생산 또는 유통하거나 이에 관련한 서비스를 제공하는 산업’으로 정의하고 있다. 또한, 과학기술정보통신부와 한국정보보호산업협회에서 2024년 10월에 발간한 「2024년 국내 정보보호산업 실태조사」에서는 정보보호산업을 ‘정보보호제품을 개발·생산 또는 유통하거나 정보보호에 관한 컨설팅, 보안관제 등 서비스를 수행하는 산업’으로 기술의 적용 영역, 제품의 특성 등에 따라 산업의 범위를 [그림 1]과 같이 정보보안, 물리보안, 융합보안으로 분류한 바 있다.

[그림 1] 정보보호산업 범위

* 출처: 한국정보보호산업협회, 「2024년 국내 정보보호산업 실태조사」

정보보호가 각종 정보데이터 및 전산망에서의 자원들을 고의적으로 또는 실수에 의한 불법적인 노출, 변조, 파괴, 서비스 지체로부터 보호이고, 개인정보는 정보보호의 대상이 되는 핵심 자원임을 고려할 때 개인정보보호산업의 개념 도출 및 범위 산정 시 정보보호산업의 개념과 범위를 포함하는 것이 타당할 것이다.

다만, 정보보안의 목표가 정보의 기밀성(confidentiality), 무결성(integrity), 가용성(availability)의 보장임을 감안할 때 가용성은 개인정보보호와는 직접적인 관련성이 상대적으로 낮다. 예를 들어, 개인정보보호의 개념에서 DDoS 대응 혹은 서버 이중화와 같은 정보통신서비스의 가용성 확보 활동은 개인정보보호 측면에서는 통상적으로 언급되지 않는 경향이 있다.

그러나, 최근에는 개인정보의 '보호'뿐 아니라 '활용'의 중요성이 높아지고 데이터 경제에서 정보주체 권리의 보장과도 밀접하게 연결되면서 가용성 역시 개인정보보호와의 관련성이 증대되고 있다. 특히, 랜섬웨어와 같이 개인정보의 접근 자체를 불가능하게 만드는 공격은 개인정보의 가용성을 직접적으로 침해하므로 개인정보 침해 사고의 일환으로 볼 수 있다.

또한, EU GDPR[1] 제32조(1)(b) 및 (c)에서도 개인정보처리의 보안조치와 관련하여 기밀성 및 무결성뿐 아니라 가용성의 보장을 직접적으로 언급하고 있다. 구체적으로, 제32조제1항은 컨트롤러 및 프로세서의 적정한 보안 수준의 보장을 위한 적정 기술적·관리적 조치의 이행 의무를 규정하고 있으며, 그 세부 조치 중 (b)호는'처리 시스템 및 서비스의 지속적인 기밀성과 무결성, 가용성, 복원력을 보장할 수 있는 역량'을, (c)호는'물리적 또는 기술적 사고가 발생하는 경우 개인정보에 대한 가용성 및 열람을 시의 적절하게 복원할 수 있는 역량'을 확보할 것을 규정하고 있다.

개인정보보호의 핵심 원칙인 정보주체의 개인정보 자기결정권의 보장은 정보보호의 개념에는 포함되지 않는 개인정보보호만의 고유한 핵심 목표이다. 더불어, 최근 AI 기술의 급속한 발전 및 보급으로 AI 학습을 위한 데이터의 중요성이 더욱 증가함에 따라 개인정보의 안전한 활용 또한 개인정보보호의 중요한 영역으로 부상하고 있다.

따라서, 개인정보보호산업은 정보주체의 개인정보 자기결정권 보장을 개인정보보호의 핵심 원칙으로 하여, 동의 절차 혹은 개인정보 처리방침 관리 등 법적 의무 이행을 위한 정책적

1) EU GDPR(General Data Protection Regulation, 일반 개인정보 보호법): 유럽 연합(EU)의 개인 프라이버시 및 개인정보보호에 대한 기본 권리를 보호하는 규정

보호 활동 지원 산업을 중심으로 구성할 수 있다. 여기에 개인정보 강화기술(PET, Privacy Enhancing Technology) 등 개인정보의 안전한 활용을 위한 산업과 정보자산으로서의 개인정보에 대한 기밀성·무결성·가용성 보장을 위한 정보보호산업을 포함할 수 있다.

이와 같이, 개인정보보호 관련 분야의 연구에 있어서 정보보호 분야와 비교·분석하는 접근법은 이전에도 다수 이루어진 바 있다. 개인정보보호위원회(이하 '개인정보위')가 2023년 1월 발간한 「개인정보 보호·활용 기술 표준화 로드맵 2023-2027」에서도 개인정보 보호·활용 기술과 정보보안 기술을 비교·분석하여 개인정보 보호·활용 기술을 표준화하고 로드맵을 도출하였다.

[그림 2]와 같이, 동 로드맵에서는 정보보안 기술의 주요 보호대상은 ICT 인프라로, 그 목적은 시스템의 기밀성·무결성·가용성을 보장하는 것이다. 이에 따라, 기술 개발 방향도 시스템 보호 중심으로 설정된다. 반면, 개인정보 보호·활용 기술의 보호대상은 정보주체이고 목적 또한 주요 정보주체의 권리 보장에 있다. 따라서, 기술 개발 방향은 개인정보의 보호와 안전한 활용에 중점을 두며, 수집-이용-저장-제공-파기의 개인정보 생명주기를 주요 프레임워크로 삼는다. 특히, 개인의 동의·선호 관리 등 정보주체의 권리보호를 위한 기술은 정보보안 기술에 포함되지 않는 개인정보 보호·활용 기술의 고유 영역에 해당한다.

[그림 2] 개인정보 보호·활용 기술과 정보보안 기술 비교

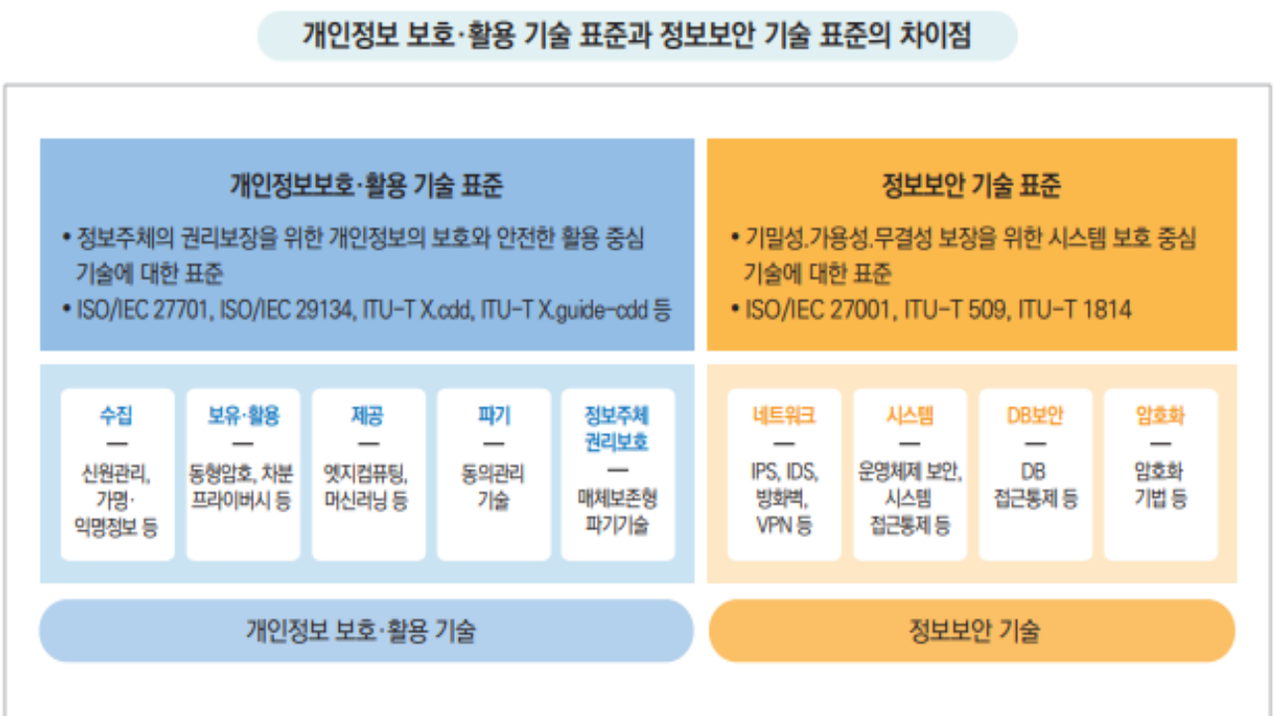
개인정보 보호·활용 기술과 정보보안 기술 비교

구 분	개인정보 보호·활용 기술	정보보안 기술
주요 보호대상	정보주체	ICT 인프라
보호 목적	정보주체의 권리 보장	기밀성, 무결성, 가용성 보장
기술개발 방향	개인정보의 보호와 안전한 활용 중심	시스템 보호 중심
프레임워크	수집-이용-저장-제공-파기	탐지-분석-대응-공유
정보주체 우선	O	X
보호를 위한 주요 탐지 정보	개인정보	일반 정보

* 출처: 개인정보보호위원회, 「개인정보 보호·활용 기술 표준화 로드맵 2023-2027」

또한, [그림 3]과 같이 개인정보 보호·활용 기술 표준과 정보보안 기술 표준의 차이점에 대한 분석에서도 정보보안 기술 표준은 네트워크·시스템·DB 등 ICT 인프라 보호 중심의 표준 개발이 중심이다. 반면, 개인정보 보호·활용 기술 표준은 정보주체의 권리 보장과 개인정보의 보호와 안전한 활용 기술 중심의 표준 개발이 핵심이라고 정리되고 있다. 기술 표준과 산업은 밀접한 관련이 있으므로 이러한 차이는 정책 및 산업 발전 측면에서도 유의미하게 고려할 필요가 있다.

[그림 3] 개인정보 보호·활용 기술과 정보보안 기술 표준의 차이점



* 출처: 개인정보보호위원회, 「개인정보 보호·활용 기술 표준화 로드맵 2023-2027」

이와 같은 분석 결과를 기반으로 개인정보위는 개인정보 보호·활용 기술 표준 분류체계를 [그림 4]와 같이 '정보주체 권리보장', '처리단계별 보호 강화', '안전한 활용' 등 3개의 중분류로 구분하고 총 17개의 소분류를 제시하였다.

[그림 4] 개인정보 보호·활용 기술 표준 분류체계

개인정보 보호·활용 기술 표준 분류체계

중분류(3)	소분류(17)	개 념
1 정보주체 권리보장	1-1. 정보주체 권리보장 체계	▸ 개인정보보호에 있어서 정보주체의 권리를 보장하는 체계에 관련된 표준
	1-2. 정보주체 동의	▸ 개인정보처리자가 법령에 따라 정보주체의 수집·동의 처리 요구를 보장하는 표준
	1-3. 정보주체 통제권	▸ 정보주체 스스로 자신의 개인정보를 직접 관리·통제하는 표준
	1-4. 정보주체 신원인증 정보관리	▸ 정보주체의 본인 여부 확인 등 인증·관리를 위한 표준
	1-5. 개인정보 침해대응	▸ 개인정보의 유·노출, 오·남용 등 침해사고 예방 및 대응을 위한 표준
2 처리단계별 보호 강화	2-1. 처리단계별 보호 강화 체계	▸ 개인정보의 수집, 저장, 이용, 파기를 통해 개인정보를 관리하는 체계 관련 표준
	2-2. PbD 원칙을 적용한 기획·설계	▸ 개인정보처리시스템 등의 기획·설계 시 사전에 개인정보 침해 위험성을 평가하는 표준
	2-3. 수집	▸ 각종 서비스에서 활용되는 다양한 데이터 유형의 수집에 관련된 표준
	2-4. 이용·제공	▸ 개인정보의 이용 및 제공 단계에서 법규에 따른 개인정보의 관리 표준
	2-5. 파기	▸ 안전한 개인정보 삭제와 저장매체 파기를 위한 표준
	2-6. 안전성확보	▸ 개인정보의 안전한 관리를 위한 기술적·물리적 보호조치 표준
3 안전한 활용	3-1. 안전한 활용 체계	▸ 개인정보의 가명·익명 처리 등 안전 활용을 위한 체계에 관련된 표준
	3-2. 기반기술	▸ 개인정보 안전 활용을 위한 개인정보 처리 지원 표준
	3-3. 서비스 응용	▸ 서비스 제공을 위해 개인정보 노출을 최소화 하면서 서비스에 필요한 개인정보를 처리·활용하는 표준
	3-4. 마이데이터 개인정보보호	▸ 정보주체가 전송을 요구하여 제공받은 본인의 개인정보를 저장하는 데이터와 관련된 서비스 및 기능에 대한 표준
	3-5. 융합 프라이버시 보호	▸ 분야별 특성을 반영한 프라이버시 보호 및 활용 표준
	3-6. 인공지능 서비스 프라이버시 보호	▸ 인공지능 활용 서비스의 프라이버시 보호 기술과 인공지능을 프라이버시 보호에 적용하기 위한 표준

* 출처: 개인정보보호위원회, 「개인정보 보호·활용 기술 표준화 로드맵 2023-2027」

첫째, '정보주체 권리보장' 분야는 정보주체 권리보장 체계, 정보주체 동의, 정보주체 통제권, 정보주체 신원인증 정보관리, 개인정보 침해대응으로 구성된다.

둘째, '처리단계별 보호 강화' 분야는 처리단계별 보호 강화 체계, 개인정보보호 중심 설계(PbD, Privacy by Design) 원칙[2]을 적용한 기획·설계, 수집, 이용·제공, 파기, 안전성 확보로 구성된다. 생명주기별 표준을 보다 구체적으로 살펴보면, 수집 단계는 각종 서비스에서 활용되는 다양한 데이터 유형의 수집에 관련된 표준이며, 개인정보의 이용 및 제공 단계는 법규에 따른 개인정보의 관리 표준, 파기 단계는 안전한 개인정보 삭제와 저장매체 파기를 위한 표준, 안전성확보 단계는 개인정보의 안전한 관리를 위한 기술적·물리적 보호 조치 표준을 의미한다.

셋째, '안전한 활용' 분야는 개인정보의 가명·익명처리 등 안전 활용을 위한 체계에 관련된 표준인 '안전한 활용 체계', 개인정보 안전 활용을 위한 개인정보 처리 지원 표준인 '기반기술', 서비스 제공을 위해 개인정보 노출을 최소화 하면서 서비스에 필요한 개인정보를 처리·활용하는 표준인 '서비스 응용' 등으로 분류된다. 또한, 정보주체가 전송을 요구하여 제공받은 본인의 개인정보를 저장하는 데이터와 관련된 서비스 및 기능에 대한 표준 '마이데이터 개인정보보호', 분야별 특성을 반영한 프라이버시 보호 및 활용 표준인 '융합 프라이버시 보호', 인공지능 활용 서비스의 프라이버시 보호 기술과 인공지능을 프라이버시 보호에 적용하기 위한 표준인 '인공지능 서비스 프라이버시 보호'도 이에 해당한다.

앞서 개인정보위의 개인정보 보호·활용 기술 표준화 로드맵에서 제시하였듯이 개인정보보호 영역에서는 개인정보 생명주기가 주요 프레임워크이다. 정보보호 및 개인정보보호 관리체계 인증에서도 개인정보 생명주기는 정보보호 관리체계(ISMS)[3] 인증과 정보보호 및 개인정보보호 관리체계(ISMS-P)[4] 인증을 구분하는 주요 기준이다.

2) 개인정보보호 중심 설계(PbD, Privacy by Design) 원칙: 개인정보 보호를 시스템 설계 단계부터 내재화하는 원칙
3) 정보보호 관리체계(ISMS): 정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 제도
4) 정보보호 및 개인정보보호 관리체계(ISMS-P): 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 제도

[그림 5] 정보보호 및 개인정보보호 관리체계 인증 기준 개요

* 출처: 개인정보보호위원회, 「정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증기준 안내서」

정보보호 및 개인정보보호 관리체계(ISMS-P)는 크게 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항', '3. 개인정보 처리 단계별 요구사항' 3개 영역에서 총 101개의 인증기준으로 구성되어 있다. 정보보호 관리체계(ISMS) 인증을 받고자 하는 신청기관은 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항' 2개 영역에서 80개의 인증기준을 적용받게 되며, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 신청기관은 '3. 개인정보 처리 단계별 요구사항'을 포함하여 101개의 인증기준을 적용받게 된다.

정보보호 및 개인정보보호 관리체계(ISMS-P)의 개인정보처리단계별 요구사항의 인증기준 또한 개인정보 생명주기와 정보주체 권리보호를 포함하여 분류된 바 있다. 따라서, 개인정보보호산업의 분류에 있어서도 이와 같은 분류 기준을 참조하여 개인정보 생명주기 및 정보주체 권리를 포함하여 분석하고자 한다.

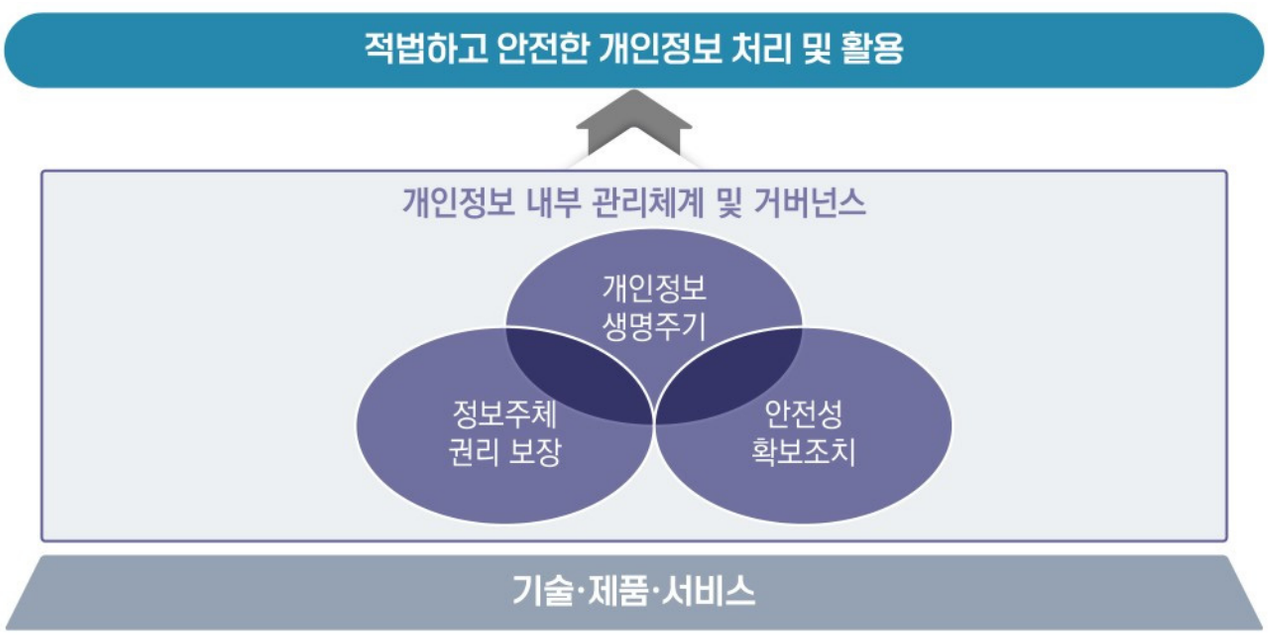
정보보호산업에 대한 기존 법제도적 개념 및 분석 자료, 개인정보보호에 대한 최근 연구 및 분석 동향을 고려할 때, 개인정보보호는 정보보호의 단순한 하위 범주가 아닌 독립된 영역으로 발전 중에 있다. 또한, 정보보호가 시스템·데이터의 기밀성, 무결성, 가용성 보장을 주목적으로 하는 반면, 개인정보보호는 생명주기를 중심으로 정보주체의 자기결정권 보장

이라는 권리 중심 접근이 핵심이다. 특히, AI 시대에는 데이터 활용의 중요성과 더불어 안전한 활용 기술(PET 등)도 산업의 중요한 축이 되고 있다.

따라서, 개인정보보호산업이란 정보주체의 개인정보 자기결정권 보장이라는 대원칙 하에, 개인정보의 적법하고 안전한 처리 및 활용을 목표로, 개인정보 생명주기에 기반한 개인정보 보호 활동(compliance), 정보주체 권리 보장 조치, 안전성 확보조치의 이행과 이를 위한 내부 관리체계 및 거버넌스 구축을 보장하는 일련의 기술·제품·서비스 산업군을 의미한다고 볼 수 있다.

이와 같은 개념을 기반으로 개인정보보호산업의 구조를 [그림 6]과 같이 정리하였다.

[그림 6] 개인정보보호산업의 개념 및 구조



* 출처: 저자 정리

개인정보 생명주기에 기반한 개인정보보호 활동, 정보주체 권리보장, 안전성 확보조치 등 세 가지 영역의 조치 사항은 서로 중첩되는 영역도 있으며 단독으로 존재하기도 한다. 예를 들면, 정보주체 권리보장을 위한 개인정보 처리방침의 수립은 정보주체의 알 권리 보장을 위한 것이기도 하나 「개인정보 보호법」에 따른 법적 의무 이행을 위한 개인정보보호 활동이다. 그러나, 아동이 이해하기 쉬운 별도의 개인정보 처리방침의 수립은 법적 의무 이행을 위한 개인정보보호 활동은 아니나 정보주체의 권리를 보다 효과적으로 보장하기 위한 권고 사항의 일환이다.

또한, 정보보호 영역은 개인정보 안전성 확보조치의 일환으로 포섭되며 네트워크, 시스템, DB 보안, 암호화 등의 정보보안 영역으로 구분되고 생명주기 전반에 적용된다. 예를 들면, 암호화 중 전송 구간 암호화는 개인정보 수집 단계에서 정보주체가 입력한 개인정보가 개인정보처리자의 시스템에 전송되는 구간에 대한 암호화 통신에도 적용되며, 이용 단계에서 DB 내에 개인정보를 암호화 저장하는 단계에도 적용되는 것이다. 정보보안이 정보자산의 보호라는 점을 고려할 때, 주로 수집 이후 이용·활용 단계에서 대부분 적용된다. 다만, DDoS, 서버 이중화 등의 일부 가용성 보장에 대한 사항은 개인정보보호와의 관련성이 상대적으로 낮아 제외된다고 볼 수 있다.

그 밖에, 개인정보 생명주기에 따른 개인정보보호 활동, 정보주체의 권리 보장, 안전성 확보조치 전 영역을 포함하여 개인정보 내부 관리체계 및 거버넌스를 구축하는 분야 또한 개인정보보호의 주요 영역으로 이를 지원하는 다양한 기술·제품·서비스가 이미 시장에 출시되어 있다.

2. 개인정보보호산업의 범위 및 분류

개인정보보호산업의 개념을 기반으로 개인정보보호산업의 범위를 3단계로 정리하였다. 우선 개인정보 생명주기를 중심으로 주요 영역을 도출하고, 생명주기 전반의 정보보안을 위한 안전성 확보조치, 생명주기 및 안전성 확보조치를 전체적으로 관리하는 관리체계 및 거버넌스에 대해 [표 1]과 같이 분류하였다.

[표 1] 개인정보보호산업 분류

구분			분류	
개인정보 생명주기		수집	· 정보주체 신원인증 제품(솔루션) (예시:본인확인서비스, 간편인증, 생체인식 등)	
			· 개인정보 탐지 및 비식별화 제품(솔루션)	
			· 동의 관리 기술(Consent Management Platform)	
			· 쿠키 동의 배너 생성 및 관리	
		이용·제공·활용	· 개인정보 가명·익명처리	· 개인정보 가명·익명처리 기술(PET 등)
				· 개인정보 가명·익명처리 제품(솔루션)
				· 가명·익명처리 적정성 검토
				· 가명정보 결합 및 분석
			· 대량 메시지 발송 및 관리 제품(솔루션)	
			· 수탁사 점검 및 관리	
			· 개인정보 전송요구권(마이데이터) 전송 표준 API 기술/솔루션 (개인정보 보호법, 신용정보법)	
		파기	· 동의 기반 파기 관리 솔루션	
			· 물리적 매체 파기 산업(디가우징, 디스크 분쇄)	
			· 데이터 삭제 제품(솔루션)	
			· 문서 파쇄 서비스	
	개인정보 안전성 확보조치		· 정보보안 제품(솔루션)	
			· 정보보안 관련 서비스	
			· 정보보안 기타	
			· 물리보안 제품	
			· 물리보안 관련 서비스	
개인정보 관리체계 및 거버넌스			· 공공기관 개인정보 영향평가 서비스	
			· 개인정보보호 컨설팅	
			· 개인정보보호 교육 및 훈련 서비스	
			· 법적 책임 대행 관련 서비스(국내 대리인, DPO 등)	
			· 전사 통합 개인정보 거버넌스 제품(솔루션)	
			· AI 프라이버시 리스크 관리 체계 구축	

* 출처: 저자 정리

가. 개인정보 생명주기

1) 수집 단계

앞서 개인정보위의「개인정보 보호·활용 기술 표준화 로드맵 2023-2027」및 ISMS-P 인증 심사 기준에서도 살펴 본 바와 같이 개인정보 생명주기는 개인정보보호 분야에서 기본적인 중요 분석 프레임워크이다. 이에, 개인정보보호산업에 있어서도 생명주기를 기반으로 산업체계를 분류하였다.

수집 단계는 전체 생명주기의 출발점으로 정보주체 동의 획득 등 적법한 근거로 개인정보를 최소한의 범위로 수집하는 것이 중요하다. 수집 단계에서는 서비스 이용에 필요한 개인정보를 수집하고, 이 과정에서 추후 ID/PW 분실 등 서비스 이용 과정에서 본인 확인을 위해 필요한 본인 확인 정보의 수집도 이루어진다.

또한, 14세 미만 아동의 경우 회원 가입 시 법정 대리인의 동의를 받아야 하기 때문에 정보주체에 대한 연령 확인이 필요하다. 이에, 정보주체 본인 확인 및 연령 확인을 위한 다양한 신원 인증 수단이 이용되며, 본인확인서비스가 대표적이다. 본인확인서비스는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 제23조의2에 따라 방송통신위원회가 지정한 '본인확인기관'에서 휴대폰 인증 및 아이핀(i-PIN)을 기반으로 제공되고 있다. 공동인증서(구 공인인증서), 간편인증(민간인증)도 중요 신원 인증 수단의 하나이다.

또한, 수집 단계에서는 개인정보 수집 최소화를 위해 불필요하거나 민감한 개인정보 입력을 자동으로 탐지하고 제한하는 기술 혹은 솔루션이 적용되기도 한다. 예를 들어, 온라인 서비스의 공개 게시판에 상담 혹은 문의 사항 작성 시 입력되는 텍스트 내에 주민등록번호나 휴대폰 번호와 같은 특정 유형의 개인정보 패턴을 탐지하여 입력을 제한하거나 자동으로 마스킹 처리하는 기술 등이다.

한편, 주민등록번호는 개인 식별이 가능한 강력한 식별자로 주민등록번호 법정주의에 의해 법률 근거에 의해서만 처리가 가능하다. 이에, 이동통신서비스 가입 등 본인 확인을 위한 주민등록증, 운전면허증 등의 신분증을 수집하나 개인정보 수집 최소화를 위해, 신분증 이미지 파일에서 OCR[5]을 기반으로 텍스트를 추출하여 주민등록번호 앞자리 및 성별 외 뒷자리를 자동으로 탐지하고 마스킹 처리하는 등 비식별 처리하는 기술이 적용된다.

---

5) OCR(Optical Character Recognition, 광학 문자 인식): 이미지 형태의 문서나 사진 속 글자를 컴퓨터가 인식하고 편집 가능한 디지털 텍스트로 변환하는 기술

EU GDPR에서는 쿠키를 통한 이용자 추적 및 맞춤형 정보에 대한 규제가 엄격하며, 쿠키를 통한 개인정보 수집 관련 고지 및 동의 획득을 위한 배너 구성 및 쿠키 선호설정에 대한 동의 관리 기술 또한 매우 중요하다. 동의 관리 기술(CMP, Consent Management Platform)은 정보주체로부터 법적 요건에 맞는 동의를 받고, 그 동의 내역을 저장, 변경, 철회까지 추적 관리하는 시스템이다. GDPR 제7조 등에 따라 적법성 요건(구분 동의, 사전 고지, 기록 유지 등)을 충족하는 구조로 설계되며, 이와 같은 쿠키 배너 적용 및 관리 기술은 별도의 솔루션 보다는 통합 거버넌스 솔루션 기능의 일환으로 제공되는 경우가 일반적이다.

2) 개인정보 이용·제공·활용 단계

① 개인정보 가명·익명처리

수집된 개인정보는 조직 내부적으로 정보주체가 요청한 서비스의 제공, 마케팅, 제품 추천, 이상행위 탐지, 서비스 개선 등 다양한 목적으로 활용된다. 이러한 내부적 이용 과정에서 가장 중요한 것은 최초 수집한 적법 목적 내의 이용이다. 대부분의 개인정보 수집이 동의를 기반으로 이루어져 동의 목적 외로 개인정보 이용을 위해서는 원칙적으로 정보주체의 추가적인 동의가 필요하다.

다만, 2020년 데이터 3법 개정으로 가명정보 제도가 도입되면서, 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리하는 경우, 정보주체의 추가 동의 없이도 통계작성, 과학적 연구, 공익적 기록보존 등의 목적으로 활용할 수 있는 법적 근거가 마련되었다.

개인정보위의 「가명정보 처리 가이드라인」에서는 정형·비정형 데이터에 대한 다양한 가명·익명처리 기술과 구체적인 절차를 규정하고 있다. 또한, 가명처리의 적정성 검토를 위해 최소 3명 이상의 검토 위원회 구성 및 외부 전문가를 통한 검토를 안내하고 있다. 특히, 비정형 데이터의 경우 외부 전문가를 과반 이상 포함하여 적정성 평가 위원회를 구성하는 것이 바람직하다고 안내하고 있다.

이에, 가명정보 지원 플랫폼(dataprivacy.go.kr)을 통해 가명정보 전문가 풀도 제공하고 있어 가명정보 처리 적정성 검토에 대한 전문가 시장도 형성되고 있다. 가명정보 제도 도입 후 기업, 병원, 연구기관, 공공기관 등은 가명정보를 활용한 분석·연구 기반을 확대하고

있으며, 이에 따른 가명처리 기술, 가명정보 결합 서비스, 가명처리 적정성 검증, 가명처리 등 다양한 산업이 성장하고 있다. 또한, 가명처리 및 적정성 검토를 자동화하는 등 가명처리 과정 전반을 관리하는 솔루션 제품도 시장에 출시되고 있다.

이와 같은 가명처리 및 가명정보 처리 과정에서 다양한 개인정보 강화기술(PET)이 활용된다. PET 기술은 데이터 분석 및 활용 과정에서 정보주체의 식별 가능성을 최소화하면서도 유용한 통계적 가치를 유지할 수 있도록 하는 기술군으로, 국내외 개인정보보호 가이드라인에서도 그 중요성이 강조되고 있으며 대표적인 PET 기술은 다음과 같다.

- 차분 프라이버시 (Differential Privacy): 데이터셋에 노이즈를 추가해 분석 결과에 포함된 특정 개인의 영향을 제거함으로써 익명성을 보장
- 동형암호 (Homomorphic Encryption): 암호화된 상태에서도 수학적 연산을 가능하게 하여 원본 데이터 노출 없이 분석 가능
- 영지식증명 (Zero-Knowledge Proof): 어떤 사실을 알지 못한 상태에서도 그 사실이 참임을 증명할 수 있도록 함
- 안전한 다자간 계산 (SMPC, Secure Multi-Party Computation) 및 사적집합교차 (PSI, Private Set Intersection): 서로 다른 기관 간 데이터 결합 및 공동 분석 시 개별 데이터 노출 없이 통계 분석을 가능하게 함
- 연합학습 (Federated Learning): 여러 개의 분산된 장치 또는 서버에서 데이터를 로컬로 학습시키고 결과만 중앙으로 공유하는 방식
- 합성데이터 생성 기술: 실제 데이터를 기반으로 통계적으로 유사한 가짜 데이터를 생성하여 개인정보 노출 없이 테스트·개발에 활용 가능

PET 기술은 마이데이터 산업, 의료 AI 개발, 고위험 신용평가 모델 등 민감정보 활용이 불가피한 분야에서 특히 필수적인 도구로 작용하고 있으며, 국내에서도 관련 기술에 대한 정부 R&D 및 민간 투자 확대가 이어지고 있다.

비정형 데이터에 대한 비식별 처리 기술은 정보주체 권리 요청 대응에도 활용된다. 현대 사회에서는 안전 관리 등의 목적으로 CCTV 및 블랙박스와 같은 다양한 형태의 고정형·이동형 영상정보처리기기를 이용한 영상정보가 촬영되고 있다. 수집된 영상정보에는 행인의 얼굴, 차량 번호판 등 개인 식별이 가능한 영상이 저장된다. 정보주체가 본인이 촬영된 영상정보에 대한 열람을 요구하는 경우 개인정보처리자는 이에 응해야 하나, 정보주체 외에 타인이 촬영된 경우가 빈번하다. 이러한 경우, 특정 정보주체 외에 영상 내 촬영된 다른 개인을 탐지하고 자동으로 블러 처리하는 등 비식별 처리를 하는 솔루션이 상용화 되고 있다.

② 대량 메시지 발송 및 관리 솔루션

대량 메시지 발송은 마케팅, 공지, 알림, 인증 등의 목적으로 수천~수백만 명의 정보주체에게 문자(SMS/LMS/MMS), 이메일, 알림톡, 푸시 메시지를 동시에 발송하는 행위이다. 「개인정보 보호법」제15조 및 제22조에서는 개인정보의 선택적 이용에 대해 별도 동의를 받도록 규정하고 있으며 「정보통신망법」 제50조 내지 제50의8에서는 광고성 정보 전송 시 사전 동의 의무, 수신 거부 시스템 구축, 식별 표시 의무 등을 규정하고 있다. 이에, 수신자의 동의 범위, 수신거부 권한, 수신 동의 및 거부 이력 관리, 오발송 방지, 전송 이력 관리 등의 요소가 매우 중요하다.

이와 같은 통합 메시지 발송 및 관리 솔루션의 주요 기능은 다음과 같다.

- 대량 메시지 발송 관리: 메시지 자동 발송, 템플릿 관리, 전송 통계 등 지원
- 수신자 수신 동의 및 거부 이력 관리: 각 수신자별로 동의 상태, 동의일자, 수단(SMS/Email) 등을 기록하고 변경·철회
- 광고성 정보 필터링 및 구분: 마케팅 메시지의 구분 표시(예: [광고]), 필수 고지사항(발신자, 수신거부번호 등) 자동 삽입
- 수신거부 자동 처리: 수신자가 '수신 거부' 클릭 등으로 거부 요청 시 자동으로 DB에서 수신 제외 처리 및 이력화
- 전송 로그 저장 및 감사 대응: 누구에게, 언제, 어떤 내용이 전송되었는지 기록하고, 법적 요청 또는 내부 감사를 대비한 로그 보관

③ 개인정보 수탁사 점검 및 관리

「개인정보 보호법」 제26조에 따르면, 개인정보처리자는 개인정보 처리 업무를 외부 수탁사에 위탁할 경우, 수탁자의 개인정보 처리 실태를 정기적으로 점검하고 관리해야 하며, 이를 위한 법적·기술적 보호조치, 위탁 계약서 체결, 공개 의무 등이 부과된다. 이러한 법적 요구에 따라, 조직은 수탁사에 대한 정기적인 점검 및 교육을 실시해야 하는데 외부 리소스를 활용하여 수탁사 점검 업무를 아웃소싱 주는 경우가 빈번하다.

또한, 점검 결과 도출된 개선 사항을 트랙킹하는 등 수탁사를 체계적으로 관리하기 위한 시스템 구축과도 연계된다. 수탁사별로 점검 이력과 개선 사항을 기록·관리하기 위한 것이 주요 기능이다. 점검 과정에서 수탁사를 교육하고 교육 이력을 관리하며, 계약기간 도래 시 개인정보 파기에 대한 이력 관리 기능 또한 제공될 수 있다.

④ 개인정보 전송요구권(마이데이터)

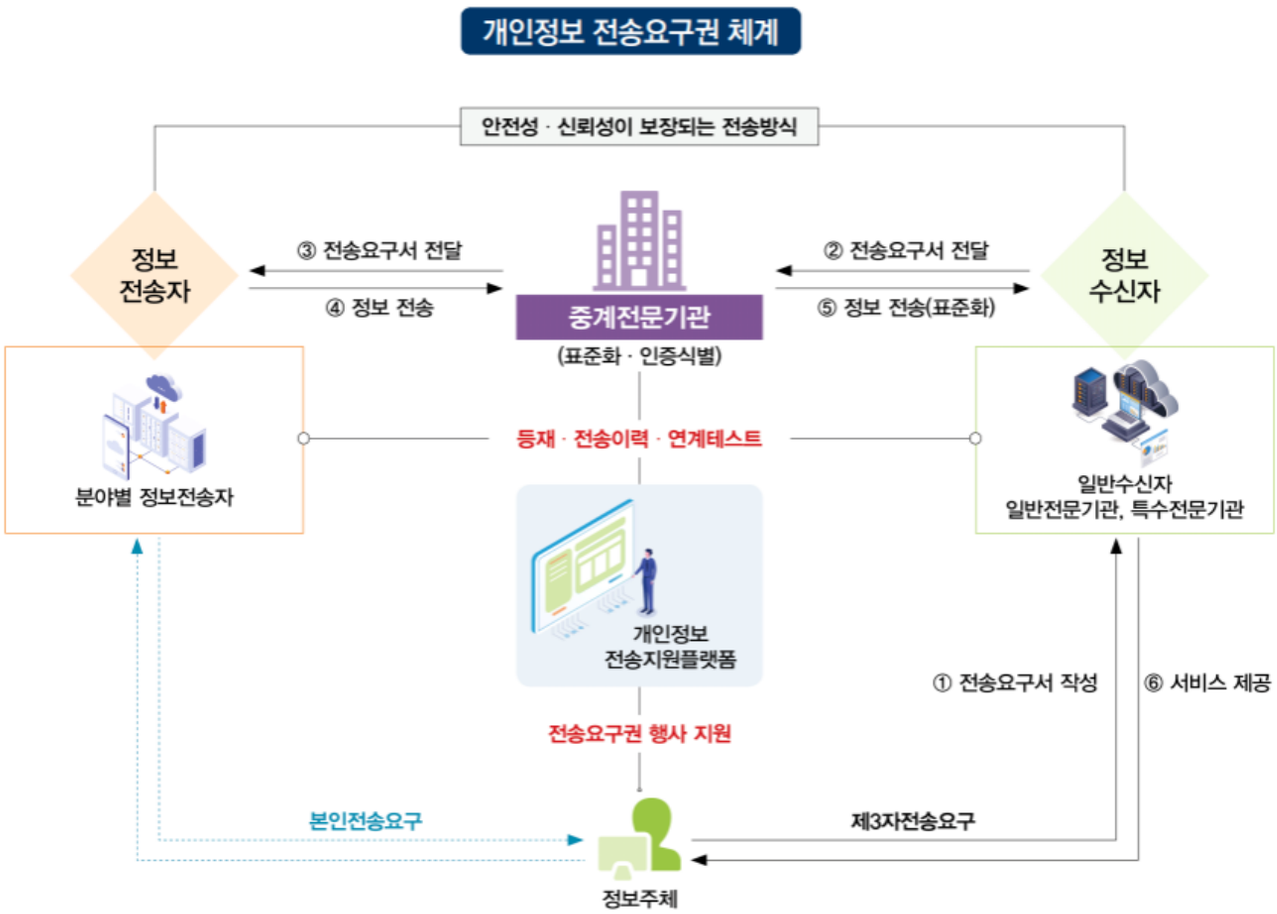
개인정보 전송요구권(마이데이터)은 정보주체가 본인에 대한 정보를 본인이 원하는 곳으로 전송 및 관리·활용하는 제도이다. 「신용정보의 이용 및 보호에 관한 법률」 개정('20년) 및 「전자정부법」 개정('21년) 을 통해 금융·공공분야에 대한 마이데이터가 개별적으로 도입되었으며, 「개인정보 보호법」 개정('23년)으로 정보주체의 일반법적 권리로서 개인정보 전송요구권이 도입됨에 따라 전 분야 마이데이터의 법적 근거를 마련하였다.

마이데이터에 대한 법제도적 정비와 함께 금융, 의료, 통신 등의 분야에서는 전송요구자에 대한 인증 절차와 표준화된 API 및 전송 이력 관리 체계를 갖춘 기술이 도입되고 있으며, 이에 따른 산업군도 성장하고 있다.

「개인정보 보호법」에 따른 전송요구권의 경우, 정보주체가 전송요구권 행사 시 이를 표준화된 API로 변환하고 인증 및 전송 내역을 관리하는 '중계전문기관', 정보주체가 전송 이력부터 철회 요청까지 한 번에 조회 가능한 '마이데이터 전송지원 플랫폼', 수신 받은 데이터를 연구 및 분석하여 정보주체가 요구한 다양한 서비스 제공에 활용하는 '정보 수신자' 등으로 구성된다.

정보 수신자 중 일반 수신자 외에 일반전문기관 및 특수전문기관 등이 있는데, 중계전문기관을 포함한 이들 전문기관은 개인정보위 및 보건복지부 등 분야별 소관 부처로부터 지정심사를 받아야 한다. 따라서, 지정심사를 위한 상시 인력풀 및 지정 심사 준비·대응을 위한 컨설팅 산업 또한 형성되고 있으며 마이데이터가 사회 전분야로 확산될 예정이므로 관련 시장 또한 성장이 예상된다.

[그림 7] 개인정보 전송요구권 체계



* 출처: 개인정보보호위원회, 「(전 분야 마이데이터) 개인정보 전송요구권 제도 안내서」

3) 파기 단계

파기 단계에서는 개인정보가 복구 또는 재생되지 않도록, 개인정보의 수집 목적이 달성되거나 법적 근거 등에 의한 보유 기간이 도래한 이후의 개인정보를 안전하게 삭제하거나 파기하여야 한다. 개인정보 파기 방식은 물리적 파기와 논리적 삭제로 나뉘며, 대상은 전자적 파일뿐 아니라 회원가입신청서 등의 종이문서, 영상기록 등 비정형 데이터도 포함된다.

전자적 형태로 저장된 개인정보의 파기는 일반적으로 데이터가 복원되지 않도록 초기화하거나 데이터 영역에 덮어쓰기를 수행하는 방식으로 이루어진다. 개인정보가 저장된 저장매체에 개인정보를 완전하게 제거하기 위해서는 저장매체의 물리적 파기가 요구되어 디가우저(Degausser)[6] 등 전용소자장비를 이용하여 삭제하거나, 디스크 분쇄기 등을 활용하여 파기한다. 이 경우, 일부 기업은 인증 받은 전문 폐기 업체에 외부 위탁하기도 한다.

그 밖에, 대규모의 종이 문서를 파기하는 경우에도 문서 파기를 전문으로 수행하는 업체를 활용하여 안전하게 파기한다. 논리적 삭제는 저장된 파일이나 DB 상의 개인정보를 복구 불가능하도록 제거하는 방식으로, 소거 알고리즘이 적용된다.

나. 안전성 확보조치

「개인정보 보호법」 제29조에 따라 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 해야 한다. 또한, 동 법 시행령 제30조에서는 법 제29조에 따라 안전성 확보조치를 규정하고 있으며 안전성 확보조치에 관한 세부기준은 「개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시 제2023-6호)」에 규정되어 있으며, 주요 내용은 정보보안산업의 주요 영역인 네트워크, DB, 암호화 등을 아우르고 있다.

이에, 안전성 확보조치의 주요 내용은 「2024년 국내 정보보호산업 실태조사」 상의 2023년 기준 정보보안 제품 및 서비스 분류와 물리보안 제품 및 서비스 분류를 기준으로 적용하는 것이 타당할 것이다.

6) 디가우저(Degausser): 자기장을 인가하여 하드디스크와 같은 저장 장치에 기록된 데이터를 물리적으로 복구 불가능하게 지우는 장치

[표 2] 정보보안산업 및 물리보안산업 분류

구분	대분류	중분류
정보보안산업	정보보안 제품(솔루션)	네트워크보안 솔루션
		엔드포인트보안 솔루션
		플렛폼/보안관리 솔루션
		클라우드보안 솔루션
		콘텐츠/데이터 보안 솔루션
		공통인프라보안 솔루션
	정보보안 관련 서비스	보안 컨설팅
		보안시스템 유지관리/보안성 지속 서비스
		보안관제 서비스
		보안 교육 및 훈련 서비스
		보안인증 서비스
	정보보안 기타	기타
물리보안산업	물리보안 제품(솔루션)	보안용카메라
		보안용 저장장치
		보안장비 부품
		물리보안 솔루션
		물리보안 주변장비
		출입통제 장비
		생체인식 보안시스템
		경보/감시 장비
		기타 제품
	물리보안 관련 서비스	출동보안 서비스
		영상보안 서비스
		클라우드 서비스
		기타 보안 서비스

* 출처: 한국정보보호산업협회,「 2024년 국내 정보보호산업 실태조사」보고서 재구성

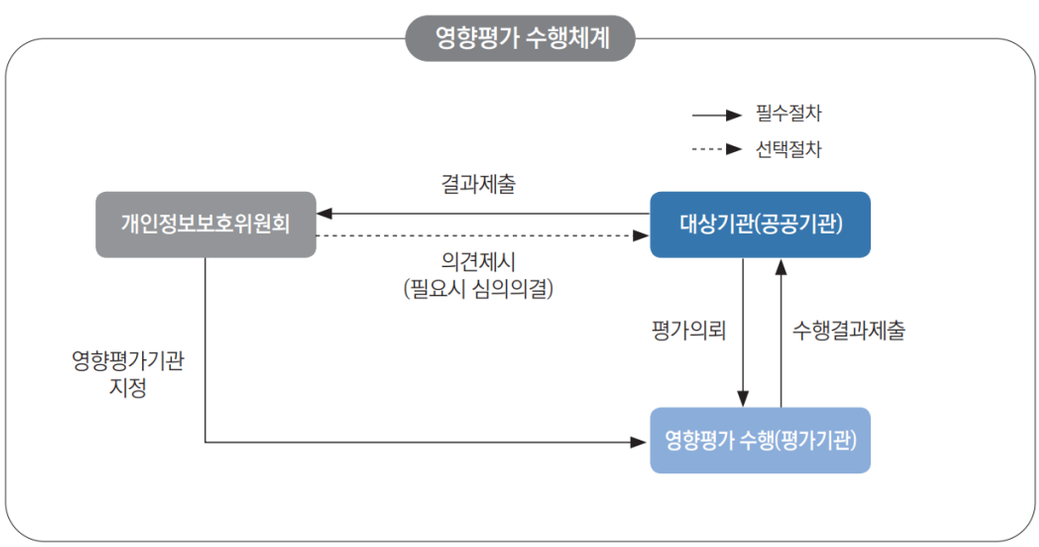
다. 개인정보 관리체계 및 거버넌스 구축

1) 공공기관 개인정보 영향평가 서비스

개인정보위에서 2024년 4월에 발간한 「개인정보 영향평가 수행안내서」에 따르면, 개인정보 영향평가는 개인정보파일을 운용하는 새로운 정보시스템의 도입이나 기존에 운영 중인 개인정보 처리시스템의 중대한 변경 시, 시스템의 구축·운영·변경 등이 개인정보에 미치는 영향을 사전에 조사·예측·검토하여 개선방안을 도출하고 이행여부를 점검하는 체계적인 절차이다.

「개인정보 보호법」 제33조 및 동 법 시행령 제35조에서는 일정 규모 이상의 개인정보를 전자적으로 처리하는 개인정보파일을 구축·운영 또는 변경하려는 공공기관에게 개인정보 영향평가를 의무화하고 있다. 또한, 「개인정보 보호법」은 개인정보위가 지정한 영향평가 기관에 평가를 의뢰하여 수행하고 그 결과 및 요약본을 최종 제출받은 날로부터 2개월 이내에 개인정보위에 제출하도록 규정하고 있다.

[그림 8] 개인정보 영향평가 수행체계



* 출처: 개인정보보호위원회, 「개인정보 영향평가 수행안내서」

따라서, 개인정보위는 「개인정보 영향평가에 관한 고시(개인정보보호위원회 고시 제2024-10호)」를 통해 개인정보 평가기관의 지정 및 영향평가의 절차에 관한 세부기준을 정하고 이에 따라 영향평가 기관을 지정하여 공고하고 있다. 이처럼, 「개인정보 보호법」 상 공공기관의 개인정보 영향평가 의무 이행 영역을 개인정보보호산업의 하위 영역으로 분류할 수 있을 것이다.

2) 개인정보보호 컨설팅 서비스

「개인정보 보호법」상 법적 의무 사항인 공공기관 개인정보 영향평가 외에도 개인정보처리자는 정보보호 및 개인정보보호 관리체계(ISMS-P), APEC CBPR[7], Global CBPR[8], ISO/IEC 27701[9] 등 개인정보보호와 관련된 다양한 국내외 인증 획득을 자율적으로 시도할 수 있다. 이와 같은 인증은 개인정보 위험을 효과적으로 관리하기 위한 내부 관리 체계 구축이 그 취지이며 상세 기준은 인증마다 상이하다. 이에, 인증에 앞서 내부적으로 개인정보 관리체계 구축을 위한 컨설팅을 수행하는 것이 일반적이다.

또한, 개인정보위에서는「개인정보 보호법」상 근거에 기반한 여러 평가제도를 운영하고 있다. 대표적으로 동 법 제11조의2 및「개인정보 보호수준 평가에 관한 고시」에 근거하여 공공기관을 대상으로 매년 개인정보보호 정책·업무 수행 및 법에 따른 의무 이행 여부 등을 평가하는 '개인정보 보호수준 평가'가 있다. 또한, 동 법 제30조의2 및「개인정보 처리방침 평가에 관한 고시」에 근거하여 개인정보처리자의 처리방침이 법에 따라 적정하게 작성되었는지, 알기 쉽게 작성되었는지 여부 등을 평가하는 '개인정보 처리방침의 평가제'가 있다. 이와 같은 평가제도에 대응하기 위해 컨설팅을 받는 경우도 있다.

이와 같이, 국내외 각종 개인정보보호 인증제도 및 법률에 규정된 평가에 대응한 개인정보보호 컨설팅 서비스 또한 개인정보보호산업의 일환으로 구분된다.

3) 개인정보보호 교육 및 훈련

개인정보보호 조치를 효과적으로 적용하려면 조직 내부 임직원뿐만 아니라 외부 수탁사 등 조직의 내외부에서 개인정보를 직접 처리하는 모든 이해관계자들의 참여가 필수불가결하다. 따라서, 모든 개인정보취급자들의 개인정보보호 인식 제고 및 역량 강화를 위한 개인정보보호 교육 및 훈련은 개인정보보호에서 매우 중요한 영역이다.

7) APEC CBPR(Cross Border Privacy Rules): 아시아-태평양 경제협력체(APEC) 회원국 간 공동의 개인정보보호 기준을 통해 자유롭게 안전한 개인정보 이전을 지원하고자 APEC 회원국 공동으로 개발한 공동 개인정보보호 인증체계
8) Global CBPR: APEC CBPR으로 시작하여 전 세계로 넓히기 위해 우리나라와 미국, 일본 등의 주도로 2022년 글로벌 협의체가 출범하였으며, 3년 간의 논의를 거친 결과 글로벌 인증(Global CBPR)을 개시함
9) ISO/IEC 27701: 개인정보보호경영시스템(PIMS, Privacy Information Management System)에 관한 국제 표준으로, 기존 ISO/IEC 27001 정보보호경영시스템(ISMS)을 기반으로 개인정보보호 관리 요구사항과 지침을 추가한 확장 규격

또한, 개인정보의 안전성 확보조치 기준 제4조제2항에서도 개인정보처리자의 개인정보보호 교육 의무를 규정하고 있다. 개인정보처리자는 교육목적 및 대상, 교육 내용, 교육 일정 및 방법 등을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.

개인정보위에서 2024년 10월 발간한 「개인정보의 안전성 확보조치 기준 안내서」에서는 개인정보보호 교육의 시행에 있어 사내교육, 외부교육, 위탁교육 등 여러 종류가 있을 수 있으며, 조직의 여건 및 환경을 고려하여 집체 교육, 온라인 교육 등 다양한 방법을 활용할 수 있도록 안내하고 있다.

이에 따라, 이러닝 등 온라인 교육 및 오프라인을 통한 집합 교육 등 다양한 교육 콘텐츠와 채널에서 개인정보보호 교육을 제공하는 것 또한 산업화되고 있다. 이와 같은 교육 산업에는 각종 인증 심사 및 실태점검 등 외부 감사에 대비한 교육 증빙 및 이력 관리 기능 또한 포함되어 있다.

결론적으로, 임직원 등 개인정보취급자의 개인정보보호 인식과 역량을 높이기 위한 교육 및 훈련은 개인정보처리자에게 필수적인 조치이자 법적 의무이다. 이에 따라, 온라인과 오프라인의 다양한 채널과 콘텐츠를 활용하는 개인정보보호 교육 및 훈련 시장은 개인정보보호산업의 중요한 한 축을 차지하고 있다. 교육 및 훈련 전용 서비스의 형태로 제공되기도 하나, 개인정보보호 컨설팅 및 수탁사 점검과 병행하여 제공되기도 한다.

4) 법적 책임 대행 서비스(국내 대리인, DPO)

글로벌 온라인 서비스 이용이 보편화되면서, 해외 사업자가 우리 국민의 개인정보를 처리하는 경우가 많다. 그러나, 국내에 주소 또는 영업소를 두지 않고 정보통신서비스를 제공하는 해외 사업자가 정보주체의 개인정보 관련 고충처리를 위해 언어 등의 어려움 없이 편리하게 연락하고, 개인정보 침해 사고 발생 시 해외 사업자에 대한 규제 집행력을 강화할 필요성이 제기된 바 있다.

이에, 「개인정보 보호법」 제31조의2에서는 국내에 주소 또는 영업소가 없는 개인정보처리자로서 전체 매출액이 1조원 이상인 자, 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 국내 정보주체의 수가 일일평균 100만명 이상인 자 등에 대해 국내 대리인 지정을 의무화하고 있다.

이들 대리인은 개인정보 보호책임자의 업무, 개인정보 유출 등의 통지 및 신고, 개인정보위 대상 물품·서류 등의 자료제출 등을 대리하도록 규정하고 있으며, 이들 대리인은 국내에 주소 또는 영업소가 있어야 한다. 이에 따라, 주요 해외 사업자들은 외부 법무법인 혹은 별도 법인을 대상으로 국내 대리인 계약을 체결하고 있다. 다만, 해당되는 해외사업자의 수가 많지는 않아 관련 산업 분야 또한 크지는 않을 것으로 추정된다.

한편, EU GDPR 제37조 내지 제39조에서는 개인정보 보호책임자(DPO, Data Protection Officer)의 지정을 규정하고 있다. DPO는 조직의 개인정보보호 법규 준수 여부를 점검하고, 개인정보 영향평가 지원, 직원 교육, 정보주체 권리 대응, 감독기구와의 소통 등 GDPR 준수를 위한 내부 통제 및 자문 역할을 수행하는 핵심 책임자이다. 국내의 개인정보 보호책임자(CPO, Chief Privacy Officer)와 일부 유사한 점이 있으나 CPO와는 달리 외부 위탁도 가능하다. 이에, 법무법인, 개인정보보호 관련 컨설팅 회사 등에서 외부 DPO 서비스를 제공하고 관련 산업이 형성되고 있다.

5) 통합 개인정보 거버넌스 솔루션

개인정보 거버넌스 솔루션은 조직 내에서 수집, 보유, 이용, 제공, 파기되는 개인정보의 전 생명주기를 체계적으로 관리하고, 법적 요구사항과 정보주체 권리를 충족하기 위한 정책, 절차, 기술의 통합 관리 체계를 지원하는 소프트웨어 또는 클라우드 기반 플랫폼이다.

이는 단순한 보안 기능을 넘어서, 개인정보보호와 관련된 내부 통제, 감사, 리스크 관리, 문서화, 자동화된 대응 절차 등을 구현함으로써 조직의 데이터 책임성과 투명성을 제고하는 데 목적이 있다. 전통적인 정보보안 솔루션이 데이터의 기밀성, 무결성, 가용성 확보에 중점을 둔다면, 개인정보 거버넌스 솔루션은 정보주체의 권리 보호, 규제 대응, 개인정보 흐름 통제에 초점을 둔다. 즉, 데이터 자체가 아닌 데이터 처리 행위의 책임성과 적법성을 다룬다.

개인정보 거버넌스 솔루션은 다음과 같은 주요 기능을 갖추고 있으며, 대부분의 상용 솔루션은 이들을 모듈화하여 제공하고 있다.

- 개인정보 흐름 관리 및 시각화 기능: 조직 내 개인정보의 보유 위치, 이동 경로, 제3자 제공 여부, 처리 목적 등을 시각적으로 추적, 데이터 인벤토리(Data Inventory), 데이터 매핑(Data Mapping) 등의 기능으로 구현되며, AI 기반 자동 탐색(Data Discovery)을 통한 비정형 데이터를 포함

- 동의 및 선호 관리기능: 정보주체가 제공한 동의의 종류, 시점, 범위 및 철회 이력을 저장하는 기능이며, EU GDPR 등 법령별 동의 처리 요건을 설정 가능
- 개인정보 영향평가(DPIA, Data Protection Impact Assessment) 자동화: 국내 「개인정보 보호법」 상 공공기관 개인정보 영향평가 의무의 절차와는 별개로 일반적인 영향평가 방법론을 적용한 것으로 새로운 시스템 도입 또는 기존 프로세스 변경 시, 개인정보 위험도를 자동 분석하며 위험요소가 발견되면 기술적·관리적 조치 권고와 함께 문서화 기능을 제공
- 문서 및 정책 버전 관리 기능: 개인정보 처리방침, 수탁계약서, 내부규정 등의 버전 변경 기록 관리, 다국어 지원 및 사용자별 인터페이스를 제공
- 권리요구 대응 자동화: 정보주체의 열람, 정정, 삭제, 처리정지, 전송요구권 등을 자동 접수·처리, 요청 내역 및 처리 이력을 감사 로그 형태로 관리
- 감사 대응 기능: 외부 감사, 조사, 분쟁 발생 시 요구되는 기록(동의 이력, 처리방침 변경, 접근기록 등)을 자동 수집·보고서화하며, 특정 시점의 정책 스냅샷 기능, 감사 대비 사전 점검 모듈 등을 포함
- 위험평가 및 대시보드 기능: 처리 프로세스별, 시스템별, 사업부서별 개인정보 리스크 수준을 실시간으로 분석하여, 시각적 대시보드로 내부 보고 시 활용

특히 글로벌 개인정보 거버넌스 솔루션 시장은 유럽의 GDPR(2018), 미국의 CCPA(2020)[10], 중국의 PIPL(2021)[11] 등 강력한 규제 시행 이후 본격적으로 성장하였다. 기업들은 기존 보안 위주의 투자를 넘어, 데이터 거버넌스를 통해 '데이터 책임성(data accountability)'을 확보하는 방향으로 전환하고 있다. 특히, 글로벌 기업들은 내부감사 대응, 상장 요건, ESG 경영의 일환으로도 이 솔루션을 도입하고 있다.

다만, 국내 개인정보보호 법규의 적용·언어·규제 로컬라이징 문제 등으로 인해 이와 같은 글로벌 거버넌스 솔루션의 국내 이용은 상대적으로 저조한 편이나, 국내 기업에 의한 통합 거버넌스 솔루션도 지속적으로 출시되고 있다.

10) CCPA(California Consumer Privacy Act, 캘리포니아주 소비자 개인정보 보호법): 캘리포니아주 거주자의 개인 데이터를 처리하는 대부분의 기업에 적용되는 데이터 개인정보보호 법률의 일부
11) PIPL(Personal Information Protection Law, 개인정보 보호법): 중국의 첫 포괄적 개인정보 보호법으로서 열람권, 정정권, 삭제권 같은 정보주체 권리를 규정

6) 인공지능(AI) 프라이버시 거버넌스 구축 서비스

최근 인공지능(AI) 기술이 급속히 발전하면서 생성형 AI를 중심으로 AI가 개인의 일상과 사회 전반으로 빠르게 확산되고 있다. 민간과 공공에서 도메인 특성, IT 환경, 보유자원 등에 따라 AI 모델을 직접 개발하거나 기성 모델을 재학습·가공하는 등 다양한 활용 사례가 늘어나고 있다. 이 과정에서 필수적으로 수반되는 개인정보 처리 및 보호 관점에서 다양한 법적·기술적 이슈가 제기되고 있다.

이에, 국내외 개인정보보호 관련 기관에서 [표 3]과 같이 개인정보 처리 및 보호 관련 다양한 안내서를 마련·배포하여 AI 프라이버시 리스크 관리를 위한 거버넌스 프레임워크를 제시하고 있다. 국내에서는 비정형 데이터 가명처리 기준, 공개된 개인정보 처리 안내서 등이 발표되었으며, 국외에서는 NIST 프라이버시 프레임워크, UK AI 플레이북 등이 관련 지침을 제공하고 있다.

이러한 노력은 AI 개발·활용 전반에 걸쳐 개인정보보호 관점을 내재화하는 것이 중요함을 보여준다. 특히, 개인정보위에서 2025년 8월에 배포한 「생성형 인공지능(AI) 개발·활용을 위한 개인정보 처리 안내서(안)」에서는 생성형 AI의 생애주기 단계별 안전조치를 제시하고, 개인정보 보호책임자(CPO) 중심의 거버넌스 구축을 강조하고 있다.

이를 통해 기업과 기관은 AI의 목적 설정부터 적용·관리까지 전사적 차원에서 개인정보 보호를 위한 내부 관리 체계를 마련하고 감독해야 한다. 결과적으로, AI 시대의 개인정보 보호는 개별 기술적 조치를 넘어, 체계적인 거버넌스 구축과 AI 생애주기 전반에 걸친 지속적인 관리가 핵심적인 과제이다.

이와 같이, AI 기술 개발 및 활용 과정에서 발생하는 프라이버시 리스크를 관리하기 위한 거버넌스 프레임워크와 솔루션의 중요성 또한 급속히 높아지고 있다. AI 프라이버시 리스크 관리 솔루션과 AI 관련 법규 준수를 위한 컨설팅 서비스는 개인정보보호산업의 새로운 핵심 영역으로 자리 잡았다.

[표 3] 국내외 AI 개인정보 처리 및 보호 관련 안내서·참고자료

구분	제 목	주요 내용
국내	**비정형 데이터 가명처리 기준** ('24.2.)	· **이미지·영상·음성** 가명처리 기준 제시 – **의료(CT, MRI), 교통, 챗봇** 등 분야별 7종 시나리오 통해 **가명정보 활용 전 과정** 상세 안내
	공개된 개인정보 처리 안내서 ('24.7.)	· **공개된 정보**의 합법적 **처리근거 해석 제시** – '정당한 이익' 조항 충족 시 AI 개발에 활용 가능
	이동형 영상기기 안내서 ('24.10.)	· **이동형 영상기기** 촬영정보 처리**기준 제시, 자율주행차, 로봇** 등 기술 개발 지원
	합성데이터 안내서 ('24.12.)	· **분야별 데이터셋** 공개 및 합성데이터 **생성·활용 기준 제시** – **보건의료·공공안전·금융** 등 분야별 합성데이터 **활용 역생성·활용**
	AI 프라이버시 리스크 관리 모델 ('24.12.)	· **AI 유형·용례·맥락**에 따른 **AI 프라이버시 리스크 경감방안 안내** – **AI 수명주기별** 프라이버시 리스크를 **기업 스스로 평가·경감**하도록 지원
	생성형 인공지능(AI) 개발·활용을 위한 개인정보 처리 안내서(안) ('25.8.)	· **생성형 AI 수명주기**(lifecycle) **각 단계**에서의 **개인정보 처리 및 보호 이슈**를 **식별** – 각 단계별로 고려해야 할 **법적 기준** 및 **안전조치** 등을 제시
국외	**NIST Privacy Framework ver 1.1** ('25.4.)	· 국가기술표준연구소(NIST) 발간 개인정보보호 관리 체계 ※ AI 프라이버시 리스크 관리 섹션을 신설한 개정안(ver. 1.1) 공개 ('25.4.) 후 의견 수렴 통해 최종안 공개 예정(~'25.12.)
	UK AI Playbook ('25.2.)	· 공공기관이 AI를 안전하고 책임감 있게 도입·활용할 수 있도록 돕기 위한 실무지침으로, 조달·설계·데이터 관리·프라이버시 보호 등 AI 도입·운용의 전 과정에 대한 단계별 가이드라인 제공
	AI Privacy Risks & Mitigations ('25.4.)	· 개인정보보호이사회(EDPB)에서 LLM의 프라이버시 리스크를 식별·평가·완화하기 위한 종합적인 리스크 관리 방법론 제시

* 출처: 개인정보보호위원회, 「생성형 인공지능(AI) 개발·활용을 위한 개인정보 처리 안내서(안)」 기반 재구성

3. 결론

지금까지의 내용을 종합하면, 개인정보보호산업은 단순히 정보보호산업의 하위 영역으로만 볼 수 없는 독자적인 영역으로 성장하고 있음을 알 수 있다. 정보보호가 시스템과 데이터의 기밀성, 무결성, 가용성 보장을 목적으로 한다면, 개인정보보호는 개인정보 생명주기를 중심으로 정보주체의 자기결정권 보장을 핵심 가치로 삼고 있다.

특히, AI 시대에 접어들면서 개인정보보호의 중요성은 더욱 부각되고 있다. 개인정보 강화 기술(PET)과 AI 프라이버시 리스크 관리 거버넌스는 개인정보의 안전한 활용과 정보주체 권리 보호라는 두 가지 목표를 동시에 달성하기 위한 필수적인 요소로 자리 잡았다. 이처럼 개인정보보호산업은 법적 준수를 넘어, 정보주체의 권리를 보장하고 데이터의 안전한 활용을 촉진하는 미래지향적 산업으로 발전하고 있다.

2025 개인정보보호산업 직무변화 모니터링 보고서

PART.

04

직무변화 모니터링 결과

4 직무변화 모니터링 결과

개인정보보호 분야 직무맵 내 총 6개 직무를 기반으로 직무별 심층 인터뷰 및 산업현장 검증을 진행하였으며, 주요 내용은 다음과 같이 요약할 수 있다.

직무	선행요인	직무변화	필요역량	직무수준
개인정보 가명·익명처리	· 데이터 3법 개정 · 코로나 19 · 4차 산업 혁명	· 보안 체계 개편 · 제도 마련	· 데이터 분석 및 통계 · 법·제도적 이해 · 가명·익명처리 기술 · IT 및 DB 구조에 대한 이해 · 개인정보 영향평가 · 책임감 및 협업 능력	3 ~ 5수준
개인정보보호 관리	· 클라우드 서버로의 전환 · 「개인정보 보호법」 개정 · 글로벌 서비스 운영 · 원격근무 확산 · 경영진 인식 변화	· 업무 자동화 · 인증 취득 의무 강화 · 글로벌 법령 준수 · 업무 세분화 및 인력 확대	· 컴플라이언스 수립 및 운영 · 리스크 검토 및 자문 · 기술적 이해 · 보고서 작성 능력 · 커뮤니케이션 및 협업 능력	4 ~ 6수준
개인정보보호 운영	· 데이터 3법 개정 · 해외 법·제도 강화 · 기술 발전 · 개인정보 활용 증가 · 개인정보 유출 사고	· 책임 및 역할 강화 · AI 기반 체계 도입 활성화 · 자동화 시스템 적용 · 조직 구성원의 인식 개선	· 유관 법령에 대한 이해 · IT 및 시스템에 대한 이해 · AI 및 자동화 기술 · 커뮤니케이션 능력	3 ~ 5수준
개인정보보호 컨설팅	· 클라우드 서비스로의 전환 · AI 기술의 발전 · 법·제도 개정	· 고도화된 보호 조치 요구 · 평가 요소 및 대상 확대 · 컨설팅 시장의 확대	· 국내외 법령 해석과 적용 능력 · IT 및 보안 기술 지식 · 해킹 툴, 개인정보 탐지 도구 사용 · 영향평가 과정에 대한 이해	4 ~ 6수준
개인정보 이동활용관리	· 마이데이터 및 데이터 안심구역 사업 확대 · 법·제도 개정 · 개인정보 유출 사고 · 코로나 19	· 개인정보보호의 영역 확대 · 정보 제공 의무 기관 확대	· 은행 및 금융산업에 대한 이해 · 데이터 및 마이데이터 서비스에 대한 이해 · 개발 역량 · 법령에 대한 이해 · 리스크 관리 능력	3 ~ 6수준
개인정보 인증·평가	· 개인정보 유출 사고 · ESG 경영의 중요성 강화 · 법·제도 개정	· 법적 기술적 전문성 확대 · 인력 확대	· 국내외 관련 법령에 대한 이해 · 국제 표준에 대한 이해 · 커뮤니케이션 능력 · 인증 심사원 자격증 소지 · 최소 3년 이상의 실무 경력	4 ~ 7수준

1. 전문가 심층 인터뷰

가. 직무별 변화 및 인력수요

개인정보 가명·익명처리

○ 산업 및 직무 변화

데이터 3법* 개정 및 코로나19 이후 디지털 전환 가속화로 데이터의 활용 규모가 급증하고 이에 따른 SW개발자에 대한 수요가 폭발적으로 확대되었다. 이러한 환경 변화 속에서 대규모 개인정보 유출 사고가 반복됨에 따라, 「개인정보 보호법」 및 유관 제도는 지속적인 개정을 통해 규제를 강화하는 방향으로 변화하고 있다. 이에 따라, 금융·통신 등 다양한 산업 분야에서도 정보보호와 개인정보보호의 중요성이 크게 부각되고 있다.

참고

[데이터 3법] 주요 개정 사항

- 2018년 11월 15일, 정부는 데이터 활용 촉진과 개인정보 보호 강화를 목표로 '데이터 3법' 개정안을 발의하였으며, 2020년 1월 9일 국회를 통과하여 같은 해 8월 5일부터 시행되었음

* 데이터 3법: 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)」, 「신용정보의 이용 및 보호에 관한 법률(신용정보법)」을 지칭

- **주요 개정 내용**: 데이터 이용 활성화를 위한 가명정보 개념 도입, 관련 법률의 유사·중복 규정을 정비하고 추진체계를 일원화 하는 등 개인정보 보호 협치(거버넌스) 체계의 효율화, 데이터 활용에 따른 개인정보 처리자의 책임 강화, 모호한 '개인정보' 판단 기준의 명확화 등이 포함

- **「개인정보 보호법」 개정안**: 개인정보의 개념을 명확히 해서 혼선을 줄이고, 안전하게 데이터를 활용하기 위한 방법과 기준 제시, 개인정보를 식별할 수 없도록 처리한 가명정보를 도입하여, 통계 작성, 과학적 연구, 공익적 기록 보존 등의 목적으로 정보주체의 동의 없이 활용할 수 있도록 허용, 데이터 활용의 폭을 확대

- **「정보통신망법」 개정안**: 정보통신망법 내 개인정보 관련 다른 법령과의 유사·중복조항 정비와 협치(거버넌스) 개선, 개인정보보호 관련 사항은 「개인정보 보호법」으로 이관, 온라인상 개인정보보호 관련 규제와 감독 주체 '개인정보보호위원회'로 변경

- **「신용정보법」 개정**: 금융 분야에서 가명정보를 활용한 빅데이터 분석 및 이용의 법적 근거를 명확히 하고, 신용정보 관련 산업의 규제 체계를 선진화하여 데이터 경제 활성화를 도모

* 출처: 대한민국 정책브리핑(www.korea.kr), 정책자료 「데이터 3법」

이러한 변화는 기업 전반의 적극적인 **보안 체계 개편**으로 이어졌고, 일부 기업에서는 기존 정보보호 조직과 분리된 독립적인 개인정보보호 전담 부서를 신설하는 등 조직 구조상의 변화가 진행되고 있다. 또한, 개인정보보호는 특정 부서에 국한된 업무가 아닌 조직 구성원 모두가 준수해야 하는 **문화적 요소**로 확산되고 있으며, 대외적으로는 기업 신뢰성 제고와 직결되는 **ESG 경영의 핵심 가치**로 인식되고 있다.

더불어, 4차 산업혁명과 구글의 알파고 등장 이후 데이터 활용의 중요성이 본격적으로 확대되면서, 「데이터 산업진흥 및 이용촉진 기본법」 제정 등 **데이터 활용 중심의 제도 기반이 마련**되었다. 이에 개인정보보호위원회에서는 '가명정보 제도·운영 혁신방안'*을 통해 제도의 활용성과 운영 효율성을 지속적으로 개선하고 있다.

다만, 기업 현장에서는 규제 리스크에 비해 기대 수익이 충분하지 않다는 인식으로 인해 가명처리 서비스를 적극적으로 추진하는 사례가 많지는 않은 상황이다. 그럼에도 불구하고 데이터 활용과 보호의 균형을 맞추기 위한 제도적 지원은 산업 전반의 안정적 성장과 신뢰 기반 조성에 있어 중요한 역할을 수행할 것으로 판단된다.

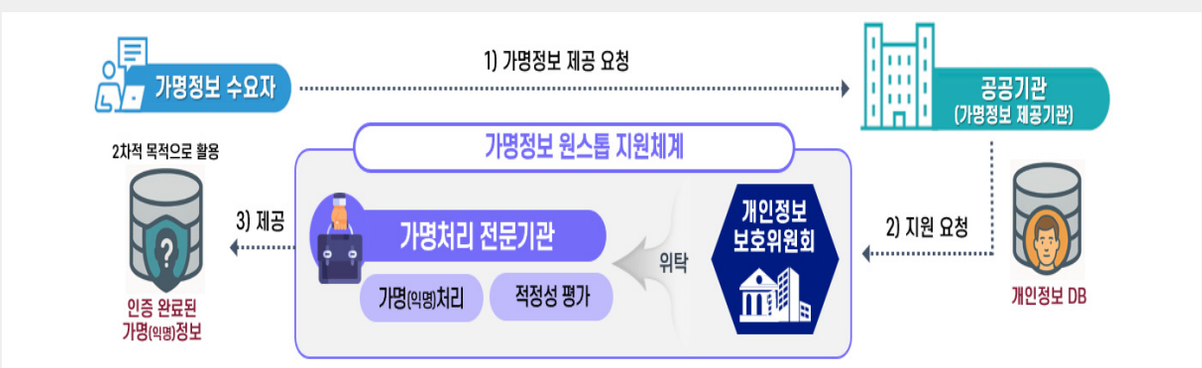
참고

[가명정보 제도·운영 혁신방안] 요약

① 공공기관 가명정보 제공 대폭 확대

- 가명처리를 위탁할 수 있는 원스톱서비스 제공
- 개인정보위가 지정한 공신력 있는 전문기관을 통해 가명처리 적정성 확인

〈 가명처리 원스톱 지원 추진체계(안) 〉



- 가명정보 제공 실적을 가점 항목으로 반영하여 가명정보 제공 유인 제공

* '가명정보 처리 수수료 가이드라인' 제시 예정

② 절차 간소화, 기간 단축

- 공공기관 내 가명정보 제공 절차 효율화

· 가명처리 절차를 차등화하여 탄력적으로 적용

〈 리스크 기반 절차 차등화 예시(안) 〉

데이터 위험도 고려요소	수신자 처리환경 취약도 고려요소
‣ 수신자가 식별할 위험이 있는 데이터 항목의 수 및 해당 데이터의 규모 ‣ 데이터 특성(예: 비정형, 특이정보) ‣ 가명처리 기술	‣ 데이터 사용목적(예: AI학습, 상품개발) ‣ 데이터 접근 제한 수준(예: 취급자 수) ‣ 처리공간 보안수준

저위험*	중위험	고위험
담당자 적정성 검토	적정성 심의 실시 (위원 2인 이상, 서면심의 가능)	적정성 심의위원회 구성 (위원 5인 이상, 서면심의 불가)

* 예: 처리기간 연장, 시계열 데이터 반복결합, 개인정보 이노베이션존 내 이용

③ **데이터 손실 최소화, 활용성 강화**

· 가명처리 적정성 심의위원회의 구성, 운영 등에 관한 사항 법제화

· 「개인정보 이노베이션존」 운영 확대·강화

④ **기타**

· 가명처리 표준화 기술 등 개인정보 안전활용 선도 기술개발 추진

· AI 중심 개인정보 특화 석·박사 과정 신설 추진

* 출처: 관계부처 합동, 「가명정보 제도·운영 혁신방안」
개인정보보호위원회(www.pipc.go.kr), 보도자료 '가명정보 활용 문턱 낮추고, 데이터 혁신 촉진한다'

특히, **신기술의 확산**은 개인정보 가명·익명처리 직무와 그 외 개인정보보호 직무 전반에 큰 영향을 미치고 있다. AI·빅데이터·머신러닝·딥러닝 등 신기술이 빠르게 발전함에 따라 개인정보를 포함한 데이터 학습 수요가 증가하였으며, 이에 따른 기술적 보호조치, 데이터 품질 검증, 학습 데이터 관리 등 개인정보보호의 기술적 요구수준도 크게 높아졌다. 이러한 급격한 기술 변화 속에서 관련 동향을 빠르게 이해하고 실무에 즉시 반영할 수 있는 역량의 중요성이 더욱 강조되고 있다.

또한, 다수의 기업이 LLM[12]을 활용한 서비스를 본격적으로 운영하기 시작하면서 데이터의 양과 활용 방식이 대폭 확대하였다. 기술 경쟁력 확보와 시장 선점을 위한 경쟁이 심화됨에 따라, 서비스 개발 속도가 가속화 되고 개발 초기 단계부터 보안 인력이 참여하는 사례가 증가하고 있으며, 데이터 보호 조치와 기술적 검토가 서비스 개발 프로세스에 필수 요소로 자리 잡아가고 있다. 이러한 변화는 개인정보보호가 **서비스 기획·개발·운영 전 과정에 걸쳐** 요구되는 요소로 발전하고 있음을 보여준다.

12) LLM(Large Language Model, 대규모 언어 모델): 대규모의 텍스트 데이터를 학습하여 자연어 이해와 생성 작업에 탁월한 성능을 보이는 심층 신경망(deep neural network) 모델

필요 역량 및 인력 수요

가명·익명처리 및 데이터 기반 개인정보보호 직무에서는 **데이터 분석과 통계적 이해**가 필수적인 역량으로 요구된다. 대규모 데이터를 처리하기 위해 다양한 데이터 처리 솔루션이 활용되고 있으며, 일부 기업에서는 자체 데이터 처리 도구를 개발하여 사용하기도 한다. 이 과정에서 반출심사 또는 리스크 진단을 위해 파이썬, R, 엑셀 등 통계 분석 도구를 활용하여 데이터를 분석하고 그 결과를 해석·활용할 수 있는 실무 역량이 요구된다.

또한, 산업별로 사용되는 데이터가 다르기 때문에 다양한 산업군에서 실제 데이터를 다뤄본 **실무 경험**이 높게 평가된다. 특히, 비정형 데이터의 비중이 증가함에 따라 이를 분석하고 처리할 수 있는 능력도 중요해졌으나, 아직 적절한 솔루션이 충분히 마련되지 않아 많은 작업이 수작업으로 이루어지고 있는 실정이다. 이에 따라, 비정형 데이터 처리 기술에 대한 꾸준한 연구개발과 투자가 필요해 보인다.

법·제도적 이해 역시 핵심 역량으로 요구된다. 「개인정보 보호법」에 대한 이해는 기본적인 전제 요건이며, 특히 가명·익명처리 과정이 많이 요구되는 의료 분야에서는 「생명윤리법」, 보건의료 데이터 활용 가이드라인 등 분야별 법령과 제도를 폭넓게 이해할 필요가 있다. 또한, 개인정보 영향평가와 같은 제도적 절차를 수행할 수 있는 역량도 필수 요건으로 간주되며, 법·제도적 준수사항과 기술적 요구사항을 통합적으로 고려할 수 있는 전문 인력에 대한 수요가 증가하고 있다. 기업의 규모에 따라서는 변호사와 협업하여 이러한 법 관련 업무 과정을 수행하기도 한다.

가명·익명처리 기술에 대한 전문적 이해도 필수 역량으로 부각되고 있다. 기존에는 법적 준수 중심 업무의 비중이 컸다면, 최근에는 해시 처리, 마스킹 및 범주화, 노이즈 추가 등 다양한 기술적 비식별 기법을 이해하고 실제 업무에 적용하는 능력이 요구되는 상황이다. 이 과정에서 가명처리 기능을 갖춘 솔루션 활용 능력도 필요하며, 가명정보의 안전성을 검토하기 위한 기술적 진단 역량도 중요해지고 있다. 더 나아가, 개인정보 처리 흐름 전반을 분석하여 위험 요소를 식별하고, 이에 적절한 보호 조치를 설계하는 능력 역시 핵심적인 직무 역량으로 자리 잡고 있다. 공공기관을 중심으로 운영되는 '가명처리 실무자 과정' 등의 외부 교육은 실무 역량 강화에 실질적인 도움이 되고 있다.

더불어, **IT 및 데이터베이스 구조에 대한 이해**도 필수적이다. 가명·익명처리 업무는 개인정보 데이터 비식별 처리 및 결합 컨설팅과 함께 수행되는 경우가 많다. 따라서, DB 구조에 대한 이해를 바탕으로 SQL 작성 능력과 Hadoop[13]과 같은 대용량 데이터 처리 기술을 보유한 인력이 선호된다. 또한, 컴퓨터 사이언스, 네트워크, 분산처리 등 IT 전반의 기본 지식과 클라우드, 빅데이터와 같은 신기술에 대한 이해도 실무에 큰 도움이 되며, 이와 관련된 수학·통계·데이터 등의 전공자와 정보보호·데이터사이언스 전공자는 직무 적응도가 높은 편이다.

가명·익명처리 직무 수행에 있어 **개인정보 영향평가 관련 자격 소지자를 우대하고 있으며,** ISMS-P, CPPG, IT·데이터 분석·통계 관련 자격증은 실무에 많은 도움을 준다. 다만, 현재 데이터 분석부터 정보보호, 법적 이해까지 통합적으로 검증하는 공신력 있는 개인정보보호 분야의 국가 자격은 아직 존재하지 않아 향후 자격제도 신설의 필요성이 제기되고 있다.

직무 수행과정에서는 **책임감과 협업 능력**도 요구한다. 법적 규제와 가이드라인을 꼼꼼하게 검토하고 전사 정책에 반영해야 하며, 특히 데이터 활용 부서에 개인정보 관련 법적 가이드를 제공하고 윤리적 인식을 제고하는 등 조직 내 가교 역할을 수행해야 한다. 데이터 활용 부서와의 적극적인 소통을 통해 보안 필요성을 설득하고 조율하는 능력은 개인정보보호 직무 전반의 핵심 역량으로 꼽힌다.

최근 다양한 개인정보 유출 및 보안 사고의 증가로 인해 보안에 대한 인식이 전반적으로 강화되고 있으며, 개인정보보호 전문 인력의 수요는 지속적으로 증가할 것으로 전망된다. 아울러, 개발자·데이터 전문 인력 양성 과정에 개인정보보호 인식을 내재화하기 위한 교육 진행 또한 산업 전반에서 중요한 과제로 부상하고 있다.

13) Hadoop(High-availability distributed object-oriented platform): 대용량 데이터 분산 처리 플랫폼의 약자로 다수의 범용 컴퓨터를 연결하여 하나의 시스템처럼 작동하도록 묶어 대용량의 다양한 데이터들을 분산 처리하는 오픈소스 프레임워크

산업 및 직무 변화

최근 기술의 고도화와 제도적, 글로벌 규제 환경 변화에 따라 업무 범위와 역할이 크게 변화하고 있다. **기술적 측면**에서는 온프레미스 중심의 인프라 구조에서 클라우드 환경으로의 전환이 본격화되면서, 트래픽 관리와 데이터 보호, 개인정보 국외 이전 등 데이터 접근 및 통제 방식이 더욱 정교해지고 있다. 또한, AI 기술 도입의 확산으로 악성 메일 분석, 취약점 탐지 등 보안 및 개인정보보호 업무의 자동화가 점차 확대되고 있다.

제도적 변화 역시 큰 영향을 미치고 있다. 「개인정보 보호법」 개정으로 규제와 처벌 기준이 강화됨*에 따라, 기업에서는 보다 체계적인 관리와 대응이 요구되고 있다. 최근 한 국내기업에서는 개인정보 유출 사고에 대해 1,000억 원 이상의 과징금을 부여받은 바 있다. 특히, 금융권에서는 「개인정보 보호법」 이외에도 금융감독원의 제재 기준과 연계된 법적 요구사항 준수가 필수적이다. 더불어, ISMS, ISO, CBPR 등 글로벌 인증제도의 확산은 기업의 개인정보 관리 체계 구축 및 인증 취득 의무를 강화하고 있다.

참고

[「개인정보 보호법」] 「개인정보 보호법 시행령」 주요 개정 사항

제63조(과태료의 부과기준) 법 제75조에 따른 과태료의 부과기준은 별표 2와 같다. **〈개정 2025. 9. 23.〉**

· '[별표2] 과태료의 부과기준(제63조 관련)' 내 항목 신설 사항

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
허. 법 제31조의2제2항을 위반하여 국내 대리인을 지정한 경우	법 제75조 제3항제3호	2,000		
고. 법 제31조의2제3항을 위반하여 국내 대리인을 관리·감독하지 않은 경우	법 제75조 제3항제4호	2,000		
노. 법 제31조의2제4항을 위반하여 국내 대리인의 성명·주소·전화번호 및 전자우편 주소를 개인정보 처리방침에 포함하지 않은 경우	법 제75조 제4항 제9호의2	200	400	800

* 출처: 국가법령정보센터(www.law.go.kr)

글로벌 서비스 운영 측면에서도 초기 개발 단계부터 미국, 유럽, 동남아, 중동 등 국가별 개인정보보호 관련 법령을 종합적으로 고려해야 하며, 현지 법률 전문가의 자문을 통해 법적 리스크를 관리하는 체계가 점차 보편화되고 있다.

이 외에도 **근무환경, 조직 구조, 업무 방식 전반에서 다양한 변화가** 나타나고 있다. 코로나19 이후 재택 및 원격근무 확산으로 보안 정책과 솔루션이 다양해졌으며, 이에 따라 보안 체계를 보다 유연하게 관리할 수 있는 역량이 중요해지고 있다. 또한, 개인정보를 단순한 관리 대상이 아닌 '리스크 관리 대상'으로 인식하는 경향이 확산됨에 따라, 조직 내 개인정보보호 관련 조직이 세분화되고 인력이 확대되고 있다. 업무 측면에서도 기존 개인정보 처리방침, 동의서 작성 중심에서 벗어나 컴플라이언스 검토, 가이드 제공 등 관리적 역할의 비중이 높아지고 있다.

○ 필요 역량 및 인력 수요

개인정보보호 관리 직무는 기업 전반의 개인정보보호 정책을 수립하고 관리 체계를 설계하는 등 **컴플라이언스 수립 및 운영** 업무를 담당한다. 기업 내부 지침과 정책을 수립하고 관련 보안 솔루션을 도입·운영하며, ISMS-P 등 인증제도 취득 및 컴플라이언스 관련 업무를 총괄한다. 또한, 임직원 업무 수행 과정에서 발생하는 개인정보보호 관련 법적 문의를 검토하고 필요시 외부 로펌과 협의하는 등 대내외 협업 역할도 수행한다. 이러한 업무 수행을 위해서는 「개인정보 보호법」, 금융위원회 가이드라인, 분쟁조정 사례 등 관련 법령과 지침을 숙지하고 이해하는 것이 필수적이다.

또한, 개인정보보호 관련 **리스크 검토 및 자문** 역할도 수행한다. 최근 개인정보보호에 대한 기업의 인식 변화로 인해 신규 서비스 기획 단계에서부터 개인정보 관련 리스크 검토 및 자문을 필수로 진행하고 있다. 스타트업과 중소기업에서도 이러한 요구가 늘어나고 있어 사업부서와의 협업 능력이 중요하다. **기술적 이해와 적용** 능력 또한 필수적이며, 해킹 및 보안 사고 대응, 인프라·보안 솔루션 운영, 네트워크·DB·클라우드 등 IT 구조 이해와 더불어 이러한 기술의 변화를 빠르게 학습하고 적용할 수 있는 역량이 요구된다.

기타 필요한 역량으로는 임원진이 이해할 수 있는 형태로 **보고서를 작성**하고, 개발자·기획자 등 다양한 부서와 원활히 소통하는 **커뮤니케이션** 능력, 프로젝트와 리스크를 관리하는 능력이 포함된다. 또한, 현재 개인정보보호 직무 담당자들은 CISSP, CPPG, CISA 등 국제·민간 자격증을 다수 보유하고 있으며, 최근 ISRM 취득 사례도 증가하고 있다. 다만, 국내

공인 개인정보보호 자격이 부재하므로 기사, 산업기사 등 국가 공인 자격 신설이 필요하다는 의견이 있다.

인력 수요 측면에서는 개인정보보호 관련 학과 개설과 전공 과목 확대 등의 정규교육 기반이 점차 마련되고 있으며, IT 기업에서도 개인정보보호 인력을 상시 채용하는 등 **수요가 꾸준히 증가**하고 있다. 그러나 7년차 이상 중·고급 경력 인력은 여전히 부족한 상황이며, 기술 중심의 교육과 더불어 실무 중심의 법·정책 사례 공유, 커뮤니케이션, 프로젝트 관리 및 리더십 교육이 확대될 필요가 있다.

개인정보보호 운영

○ 산업 및 직무 변화

데이터 3법 개정 이후 가명정보 처리 시장이 형성되면서 개인정보보호산업이 빠르게 성장하였다. 또한, **「개인정보 보호법」을 중심으로 규제와 과징금 수준**이 높아지면서 기업이 체감하는 규제 부담이 크게 증가하였다. 이에 따라, 기업 내부에서는 개인정보보호 전담 부서의 책임과 역할이 더욱 명확해졌으며, ISMS-P 등 관리체계 인증을 포함한 **법·제도적 의무 이행** 역시 강화되었다. 더불어, GDPR 등 **해외에서도 개인정보보호 관련 법제도가 강화***됨에 따라, 국내 기업의 해외 법인 운영 및 글로벌 사업 추진 과정 전반에도 직접적인 영향을 미치고 있다.

참고

[해외 개인정보보호 관련 법제도 강화] 국가별 개인정보 유출에 대한 처벌 규정

국가	주요 내용
대만	· 「개인정보 보호법」제48조제2항 및 제3항의 규정에 따라 개인정보파일을 보유한 비공공기관이 안전조치를 취하지 아니하여 개인정보가 도난·변경·훼손·파기 및 유출된 경우, **중앙목적사업주관기관 또는 직할시, 현(시)정부는 2만 신대만달러(한화 약 87만 원) 이상 200만 신대만달러(한화 약 8,700만 원) 이하의 과태료**를 부과하고, 기한 내에 시정하도록 명령한다. · **기한 내에 시정하지 아니하거나 사안이 엄중한 경우, 15만 신대만달러(한화 약 650만 원) 이상 1,500만 신대만달러(한화 약 6억 5,000만 원) 이하의 과태료**를 부과한다.
독일	· 유럽연합의 「개인정보보호규정(GDPR)」과 이를 **국내법으로 구체화한 「연방정보보호법(BDSG)」을 통해 개인정보 보호를 규율**하고 있다. · GDPR 제33조 및 제34조에 따르면, 개인정보 처리자는 개인정보 침해 사실을 인지한 때로부터 **72시간 이내에 감독기관에 이를 통지**해야 하며, 해당 침해가 자연인의 권리와 자유에 중대한 위험을 초래할 가능성이 큰 경우에는 정보주체에게도 지체 없이 알려야 한다. 통지에는 유출된 정보의 범위, 침해로 인한 예상 결과, 관련 대응 조치 등이 포함되어야 한다. · GDPR을 위반할 경우 제83조에 따라 최**대 2,000만 유로(한화 약 322억 원) 또는 전 세계 연간 총매출의 4퍼센트 중 더 큰 금액의 과징금이 부과**될 수 있다. 또한, 타인의 개인정보를 무단으로 상업적 목적으로 사용한 경우에는 BDSG 제42조에 따라 최대 **3년의 징역 또는 벌금형**에 처해질 수 있다.
미국	· 연방의 「개인정보 보호법」은 연방정부기관에 적용되는데, 연방정부가 수집하는 개인정보를 무단으로 유출하거나 법에서 정하는 관리 절차를 위반하는 행위는 경범죄이며 이와 같이 위법하게 직무를 수행한 공무원이나 직원에 대해서는 **5,000달러(한화 약 700만 원) 이하의 벌금**에 처할 수 있다. · 캘리포니아주는 「캘리포니아주 소비자개인정보보호법 2018」에서 일정 규모 이상의 사업자에게 소비자 개인정보 보호 의무를 부여한다. 해당 사업자는 그러한 정보가 유출되지 않도록 보안을 유지하는 한편, 그러한 정보를 제3자에게 제공하거나 판매할 경우에는 그 사실을 **소비자에게 사전에 고지**하고, 소비자의 자기결정권을 보호하는 조치를

국가	주요 내용
	해야 한다. 이 법을 위반하는 사업자는 그 경중에 따라 위반 **건당 2,500달러(한화 약 350만 원)에서 7,500달러(한화 약 1,000만 원) 이하의 과태료** 처분을 받을 수 있다.
프랑스	· 개인정보를 수집하는 모든 경우 유럽연합「개인정보보호규정(GDPR)」에 따라 당사자에게 정보가 수집되는 사실을 고지해야 한다. · 당사자의 동의를 구하지 않고 수집 자격이 없는 제3자에게 개인정보를 제공하는 자는「형법전」제226-22조 등에 따라 **징역 5년 및 벌금 30만 유로(한화 약 4만 8,000만 원)**에 처한다. · 이러한 정보 유출 또는 제공이 과실 또는 부주의로 일어난 경우에는 **징역 3년 및 벌금 10만 유로(한화 약 1억 6,000만 원)**에 처한다.

* 출처: 세계법제정보센터(world.moleg.go.kr), 법제동향「세계 각국의 개인정보 유출에 대한 처벌 규정」

기술 발전 역시 큰 변화를 가져왔다. 공공 및 민간 전반에서 클라우드 기반의 개인정보 처리 환경이 확산되고 있으며, AI 기술의 발전에 따라 개인정보보호 분야에서도 AI 기반 탐지·분석 체계 도입이 본격화되었다. 특히, AI 학습 데이터에 따른 비정형 데이터 관리의 중요성이 부각되면서, 로그 관리, 접근 권한 통제, 악성코드 탐지, 위협 모니터링 등 보안 운영 전반에 자동화 기술이 적용되어 업무 효율화가 이루어지고 있다. 또한, 스마트 자동차, 스마트 가전, IoT, 웰패드 등 **생활밀착형 디지털 기기에서의 개인정보의 활용이 증가**함에 따라 보호 대상 데이터 범위가 더욱 확대되고, 이에 따른 기술적·관리적 개인정보보호 요구사항도 함께 증가하고 있다.

최근 잇따른 **개인정보 유출 사고**는 기업의 인식 변화에 결정적인 영향을 미치고 있다. 사고 발생 시 대표이사의 직접적 책임 가능성이 높아지면서 최고경영진의 관심이 크게 증가하였고, 개인정보보호는 조직의 핵심 경영 리스크로 인식되기 시작했다. 이러한 변화는 탑다운 방식의 대응 강화로 이어져, 임원진 주도하에 보안 예산과 인력을 확충하는 사례가 증가하고 있으며, 조직 구성원 전반의 보안 인식 또한 빠르게 개선되고 있다.

◎ 필요 역량 및 인력 수요

개인정보보호 운영 직무를 수행하기 위해서는 법·제도에 대한 이해를 중심으로 IT·시스템 전반에 대한 지식, 기술적 보호조치 역량, 원활한 커뮤니케이션 능력, 그리고 실무 경험과 관련 자격을 종합적으로 갖추는 것이 중요하다.

법적 측면에서는 「개인정보 보호법」을 비롯하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」, 「전자상거래 등에서의 소비자보호에 관한 법률」 등 관련 주요 법령을 정확히 이해하고 이를 실제 업무에 적용할 수 있는 역량이 핵심 요건으로 작용하고 있다.

IT 및 시스템 관련 역량도 필수적이다. 개인정보 안전성 확보 조치 기준을 준수하고 적용하기 위해 IT 인프라 및 정보보호 관리 체계에 대한 이해가 필요하며, 개인정보 처리 시스템의 보안성 검토 능력도 요구된다. 최근에는 클라우드 기반 시스템 사용이 증가하면서 클라우드 관련 지식이 추가적으로 필요해지고 있다. 특히, 상용 솔루션을 활용한 모니터링이나 수탁사 관리만으로는 한계가 발생함에 따라 **기업 맞춤형 시스템 개발 능력**을 갖춘 인력에 대한 수요가 높아지고 있다. 이에 따라, IT 개발 역량과 개인정보보호 전문성을 동시에 갖춘 인력이 점점 더 중요해지고 있다.

AI와 자동화 기술 역시 개인정보보호 운영 직무의 핵심 요소로 자리 잡고 있다. 개인정보보호 업무는 지속적으로 증가하고 있는 반면, 이를 수행할 전문 인력은 상대적으로 부족한 상황에서 AI 기반 데이터 탐지·분석, 자동화 시스템 도입 등이 활발히 이루어지고 있다. 따라서, AI와 자동화 기술을 활용하여 업무 효율성을 제고할 수 있는 역량에 대한 요구도 점차 확대되고 있는 추세이다.

커뮤니케이션 능력 또한 직무 수행을 위한 핵심 요소이다. 개인정보보호 업무는 조직 전반에 걸친 협업을 전제로 하여 타부서와의 소통이 필수적이며, 개인정보보호 가이드 및 기준을 수립한 이후 이를 각 부서에 공유하고 조율하는 과정이 수반된다. 따라서, 타부서와 원활하게 소통하여 업무를 추진할 수 있는 커뮤니케이션 능력이 매우 중요하다.

개인정보보호 운영 직무에서는 CPPG, 정보보안기사, PIA, ISMS, ISMS-P 등 관련 자격 보유자가 우대되지만, 채용 시에는 자격 요건보다 2~3년 이상의 실무 경험을 갖춘 인력을 선호하는 등 **업무 수행 경험**이 중요하게 평가되는 경향이 있다. 한편, 관련 자격증은 입사 이후 기업의 지원을 통해서도 취득이 가능하며, 기업 내부적으로는 ISO/IEC 27001 등 국제 표준 교육과 최신 트렌드 세미나 등 **외부 전문 교육 참여**도 적극 권장하고 있다.

산업 및 직무 변화

AI, 블록체인, 클라우드 등 **신기술의 급격한 발전**은 개인정보보호산업 전반에 큰 변화를 초래하고 있다. 특히, **시스템 환경이 클라우드 중심으로 전환**되면서, 클라우드 환경에서 저장·처리되는 대규모 개인정보에 대한 관리 및 보호 요구 수준이 크게 높아지고 있다. 이러한 변화에 따라 기존의 서버 중심 보안 체계를 넘어, 클라우드 환경 전반에 대한 정교한 개인정보 탐지, 유출 방지 및 규제 준수 체계 구축이 필수적인 과제로 부상하고 있다.

이와 함께 AI 기술이 개인정보 탐색 및 보호 솔루션 자동화에 활용되면서, 개인정보보호 담당자의 업무 범위는 기존의 법·컴플라이언스 중심에서 기술 기반 검토 영역으로 확대되고 있다. 과거에는 법적 기준에 따른 단순한 데이터 처리 검토 수준에 머물렀다면, 현재에는 모델 학습과정에서 활용되는 개인정보에 대한 가명처리, 비식별화 등 고도화된 보호 조치가 필요해졌다. 특히, 2026년 시행 예정인 「AI 기본법」*으로 인해 기업의 서비스 운영 방식과 개인정보 보호조치 체계에 상당한 변화가 예상된다. 이에 따라 중견 이상의 기업에서는 개인정보보호 전담 인력을 적극적으로 채용하는 추세이다.

참고

[「AI 기본법」] 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 주요 내용

□ **주요 동향**

구분	제정안 의결	제정	시행
시행일자	2024. 12. 26.	2025. 1. 21.	2026. 1. 22.

□ **주요 내용**

조항	내용
제1조 (목적)	이 법은 인공지능의 건전한 발전과 신뢰 기반 조성에 필요한 기본적인 사항을 규정함으로써 국민의 권익과 존엄성을 보호하고 국민의 삶의 질 향상과 국가경쟁력을 강화하는 데 이바지함을 목적으로 한다.
제4조 (적용범위)	① 이 법은 국외에서 이루어진 행위라도 국내 시장 또는 이용자에게 영향을 미치는 경우에는 적용한다. ② 이 법은 국방 또는 국가안보 목적으로만 개발·이용되는 인공지능으로서 대통령령으로 정하는 인공지능에 대하여는 적용하지 아니한다.

조항	내용
제6조 (인공지능 기본 계획의 수립)	① 과학기술정보통신부장관은 관계 중앙행정기관의 장 및 지방자치단체의 장의 의견을 들어 3년마다 인공지능기술 및 인공지능산업의 진흥과 국가경쟁력 강화를 위하여 인공지능 기본계획(이하 "기본계획"이라 한다)을 제7조에 따른 국가인공지능위원회의 심의·의결을 거쳐 수립·변경 및 시행하여야 한다. 다만, 기본계획 중 대통령령으로 정하는 경미한 사항을 변경하는 경우에는 그러하지 아니하다.
제13조 (인공지능기술 개발 및 안전한 이용 지원)	③ 정부는 제2항에 따른 사업의 결과를 누구든지 손쉽게 이용할 수 있도록 공개하고 보급하여야 한다. 이 경우 기술을 개발한 자를 보호하기 위하여 필요한 경우에는 보호기간을 정하여 기술사용료를 받을 수 있게 하거나 그 밖의 방법으로 보호할 수 있다.
제27조 (인공지능 윤리 원칙 등)	① 정부는 인공지능윤리의 확산을 위하여 다음 각 호의 사항을 포함하는 인공지능 윤리원칙(이하 "윤리원칙"이라 한다)을 대통령령으로 정하는 바에 따라 제정·공표할 수 있다. 1. 인공지능의 개발·활용 등의 과정에서 사람의 생명과 신체, 정신적 건강 등에 해가 되지 아니하도록 하는 안전성과 신뢰성에 관한 사항 2. 인공지능기술이 적용된 제품·서비스 등을 모든 사람이 자유롭고 편리하게 이용할 수 있는 접근성에 관한 사항 3. 사람의 삶과 번영에의 공헌을 위한 인공지능의 개발·활용 등에 관한 사항
제29조 (인공지능 신뢰 기반 조성을 위한 시책의 마련)	정부는 인공지능이 국민의 생활에 미치는 잠재적 위험을 최소화하고 안전한 인공지능의 이용을 위한 신뢰 기반을 조성하기 위하여 다음 각 호의 시책을 마련하여야 한다. 1. 안전하고 신뢰할 수 있는 인공지능 이용환경 조성 2. 인공지능의 이용이 국민의 일상생활에 미치는 영향 등에 관한 전망과 예측 및 관련 법령·제도의 정비 3. 인공지능의 안전성·신뢰성 확보를 위한 안전기술 및 인증기술의 개발 및 확산 지원 4. 안전하고 신뢰할 수 있는 인공지능사회 구현 및 인공지능윤리 실천을 위한 교육·홍보 5. 인공지능사업자의 안전성·신뢰성 관련 자율적인 규약의 제정·시행 지원 6. 인공지능사업자, 이용자 등으로 구성된 인공지능 관련 단체(이하 "단체등"이라 한다)의 인공지능의 안전성·신뢰성 증진을 위한 자율적인 협력, 윤리지침 제정 등 민간 활동의 지원 및 확산 7. 그 밖에 인공지능의 안전성·신뢰성 확보를 위하여 대통령령으로 정하는 사항
제31조 (인공지능 투명성 확보 의무)	① 인공지능사업자는 고영향 인공지능이나 생성형 인공지능을 이용한 제품 또는 서비스를 제공하려는 경우 제품 또는 서비스가 해당 인공지능에 기반하여 운용된다는 사실을 이용자에게 사전에 고지하여야 한다. ② 인공지능사업자는 생성형 인공지능 또는 이를 이용한 제품 또는 서비스를 제공하는 경우 그 결과물이 생성형 인공지능에 의하여 생성되었다는 사실을 표시하여야 한다.
제32조 (인공지능 안전성 확보 의무)	① 인공지능사업자는 학습에 사용된 누적 연산량이 대통령령으로 정하는 기준 이상인 인공지능시스템의 안전성을 확보하기 위하여 다음 각 호의 사항을 이행하여야 한다. 1. 인공지능 수명주기 전반에 걸친 위험의 식별·평가 및 완화 2. 인공지능 관련 안전사고를 모니터링하고 대응하는 위험관리체계 구축 ② 인공지능사업자는 제1항 각 호에 따른 사항의 이행 결과를 과학기술정보통신부장관에게 제출하여야 한다.

조항	내용
제33조 (고영향 인공지능의 확인)	① 인공지능사업자는 인공지능 또는 이를 이용한 제품·서비스를 제공하는 경우 그 인공지능이 고영향 인공지능에 해당하는지에 대하여 사전에 검토하여야 하며, 필요한 경우 과학기술정보통신부장관에게 고영향 인공지능에 해당하는지 여부의 확인을 요청할 수 있다. ③ 과학기술정보통신부장관은 고영향 인공지능의 기준과 예시 등에 관한 가이드라인을 수립하여 보급할 수 있다.
제34조 (고영향 인공지능과 관련한 사업자의 책무)	① 인공지능사업자는 고영향 인공지능 또는 이를 이용한 제품·서비스를 제공하는 경우 고영향 인공지능의 안전성·신뢰성을 확보하기 위하여 다음 각 호의 내용을 포함하는 조치를 대통령령으로 정하는 바에 따라 이행하여야 한다. 1. 위험관리방안의 수립·운영 2. 기술적으로 가능한 범위에서의 인공지능이 도출한 최종결과, 인공지능의 최종결과 도출에 활용된 주요 기준, 인공지능의 개발·활용에 사용된 학습용데이터의 개요 등에 대한 설명 방안의 수립·시행 3. 이용자 보호 방안의 수립·운영 4. 고영향 인공지능에 대한 사람의 관리·감독 5. 안전성·신뢰성 확보를 위한 조치의 내용을 확인할 수 있는 문서의 작성과 보관 6. 그 밖에 고영향 인공지능의 안전성·신뢰성 확보를 위하여 위원회에서 심의·의결된 사항
제35조 (고영향 인공지능 영향평가)	① 인공지능사업자가 고영향 인공지능을 이용한 제품 또는 서비스를 제공하는 경우 사전에 사람의 기본권에 미치는 영향을 평가(이하 "영향평가"라 한다)하기 위하여 노력하여야 한다. ② 국가기관등이 고영향 인공지능을 이용한 제품 또는 서비스를 이용하려는 경우에는 영향평가를 실시한 제품 또는 서비스를 우선적으로 고려하여야 한다. ③ 그 밖에 영향평가의 구체적인 내용·방법 등에 관하여 필요한 사항은 대통령령으로 정한다.
제36조 (국내대리인 지정)	① 국내에 주소 또는 영업소가 없는 인공지능사업자로서 이용자 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 자는 다음 각 호의 사항을 대리하는 자(이하 "국내대리인"이라 한다)를 서면으로 지정하고, 이를 과학기술정보통신부장관에게 신고하여야 한다. 1. 제32조제2항에 따른 이행 결과의 제출 2. 제33조제1항에 따른 고영향 인공지능 해당 여부 확인의 요청 3. 제34조제1항 각 호에 따른 안전성·신뢰성 확보 조치의 이행에 필요한 지원(같은 항 제5호에 따른 문서의 최신성·정확성에 대한 점검을 포함한다) ② 국내대리인은 국내에 주소 또는 영업소가 있는 자로 한다. ③ 국내대리인이 제1항 각 호와 관련하여 이 법을 위반한 경우에는 해당 국내대리인을 지정한 인공지능사업자가 그 행위를 한 것으로 본다.

* 출처: 국가법령정보센터(www.law.go.kr)

또한, AI 기술의 영향력이 두드러지면서 '개인정보 영향평가'와 '개인정보 관리 체계'에도 새로운 요소들이 도입되고 있다. 「개인정보 보호법 시행령」 개정과 함께 AI 관련 요소가 평가 기준에 포함되면서, 프라이버시를 고려하여 시스템을 설계하는 'PbD'의 필요성도 높아지고 있다. 이러한 업무는 개발자만의 역할로 한정되기 어려워, 개인정보보호 및 정보보호 부서가 개발 단계부터 적극적으로 참여해야 하며 그 업무 범위도 점차 확대될 것으로 예상된다.

법·제도 환경 변화에 따라 개인정보보호 평가의 적용 범위는 지속적으로 확대되고 있다. 공공기관과 지방자치단체는 매년 '개인정보 보호 수준평가'를 의무적으로 수행해야 하며, 최근 시행령 개정으로 지방자치단체의 출자·출연 기관까지 **평가 대상이 확대**되었다. 개인정보보호위원회는 향후 민간기업을 대상으로 개인정보 영향평가 적용을 점차적으로 확대할 계획을 밝힌 바 있다. 이러한 제도적 변화에 따라 공공 시스템의 안전성 확보를 목적으로 데이터베이스 보호, 접근통제, 암호화, 로그 관리, 취약점 점검 등 기술적·관리적 보호조치가 한층 강화되고 있다. 최근 증가하고 있는 해킹 및 개인정보 유출 사고는 이러한 정책 강화의 필요성을 뒷받침하는 주요 요인으로 평가된다.

개인정보보호 컨설팅 시장도 빠르게 확장되고 있다. 코로나19 이후 원격 업무가 일상화되면서 개인정보보호 검토 항목은 더욱 늘어났고, 컴플라이언스 준수 여부와 인증 관련 컨설팅 수요 역시 대폭 증가하였다. 동시에 AI 기술 발전과 강화되는 규제를 기반으로 개인정보보호 산업 자체도 활성화되고 있다. 이에 따라, AI와 클라우드 기술을 이해하고 대응할 수 있는 전문성을 바탕으로 한 컨설팅 수요가 증가하면서 담당자들의 업무 부담 역시 커지고 있다. 평가 대응, 기술 점검, 영향평가, AI 관련 검토 등 과중한 업무는 담당자들의 업무 부담으로 이어지고, 특히 중소기업에서는 이러한 업무 가중이 꾸준히 지속될 경우 이직률 증가에 따른 인력난 심화가 우려되고 있다.

필요 역량 및 인력 수요

개인정보보호 컨설팅 직무에서는 영향평가 및 공공 시스템 보호 정책 변화로 인해 관련 솔루션 시장이 확대되고 보안 기술 역량의 필요성이 꾸준히 증가하고 있다. 이러한 환경 변화 속에서 개인정보보호 담당자들이 **전문성을 강화하고 다양한 방법론을 습득**할 수 있도록 체계적인 교육의 필요성이 크게 대두되고 있다. 특히 인증·평가와 관련된 기술적 접근을 통해 개인정보보호 시스템을 설계하고 위험 요소를 사전에 대응하는 능력이 중요하게 요구되고 있다.

또한, 「개인정보 보호법」, 「정보통신망법」 등 개인정보보호 관련 법령뿐 아니라 「근로기준법」, 「금융법」, 「통신법」, 「소비자 보호법」 등 **업무와 연관된 다양한 법령을 이해**하는 것이 필요하다. 단순한 법 조항의 암기보다 조직의 서비스에 필요한 법률 해석과 적용 능력이 더욱 중요하며, 최근에는 「AI 기본법」과 해외 진출을 위한 GDPR 이해도 필수 역량으로 떠오르고 있다. 더불어, 개인정보 관련 외부 이슈를 분석해 자사 환경과 비교·점검할 수 있는 능력도 요구된다.

기본적인 **IT 및 보안 기술에 대한 지식**은 개인정보보호 업무 수행의 기반이 되는 영역으로, DB 구조와 SQL, 네트워크 이해, 서버 아키텍처, 개발 언어 등 기본적인 IT 지식은 필수적이다. 아울러 접근 제어, 암호화, 취약점 점검, 로그 관리, 침입 탐지 등 보안 기술 전반에 대한 이해가 필요하며, 최근에는 AI 모델 구조, 클라우드 보안, 블록체인, 익명화·가명화 기법, 프라이버시 강화 기술 등 신기술에 대응할 수 있는 역량이 새롭게 요구되고 있다. 또한, 개발 단계에서 개인정보보호 및 정보보호 관점에서 가이드를 제공할 수 있는 기술적 조언 능력도 필요하다.

개인정보보호 컨설팅 업무는 관리적, 법·규제 대응, 기술적 영역별 담당자로 구성된 팀 단위로 수행되는 것이 일반적이다. 현장에서는 **해킹 툴, 보안 솔루션, 개인정보 탐지 도구** 등을 활용하여 개인정보의 수집·이용·보관·제공·파기 전 과정을 단계별로 분석하고, 사고 발생 가능성이 존재하는 지점을 식별·시각화하는 능력이 요구된다. 특히, 개인정보 영향평가 수행을 위해서는 평가 방법론 이해, 리스크 도출, 완화 방안 설계 등 **영향평가 전 과정에 대한 이해**가 필요하다. 컨설팅 종료 이후에는 프로젝트 관리자가 직접 교육을 실시하거나 필요에 따라 외부 전문 강사를 연계하여 조직 내 개인정보보호 역량 강화를 지원하고 있다.

개인정보보호 컨설턴트의 경우 CPPG와 정보보안기사 등의 자격증 소유자를 우대하고 있으며, ISMS-P 인증 심사원, 개인정보 영향평가 전문가 등의 자격증은 업무 수행에 도움이 될 수 있다. 전공 배경으로는 정보보호학, 컴퓨터공학, 전산학 계열뿐만 아니라 컴플라이언스 및 법·제도 이해를 기반으로 한 법학 전공자도 폭넓게 활동하고 있다. 비전공자 역시 지속적인 학습과 자격증 취득을 통해 진입 가능하며, 신입 인력은 주로 모의해킹 및 취약점 진단 등 기술적 업무를 중심으로 실무 경험을 축적한 후, 법·규제·관리 영역으로 역할을 확대하는 경향이 나타나고 있다.

개인정보 영향평가 대상이 확대되면서 개인정보보호 컨설팅 직무에 대한 수요는 향후에도 지속적으로 증가할 것으로 예상된다. 특히 인증·평가 컨설팅, 점검·감사, 기술 기반 개인정보보호 역량을 갖춘 인력의 필요성이 더욱 커지고 있으며, 조직 내부적으로도 기술 중심의 현장 점검 능력과 시스템 기반 감사 역량 강화에 대한 요구가 확대되고 있다.

개인정보 이동활용관리

○ 산업 및 직무 변화

2021년 개인정보 자기결정권이 확대되면서 **마이데이터 사업***이 본격적으로 도입되었으며, 금융권을 중심으로 마이데이터 사업자 등록을 통해 자사 애플리케이션에서 이용자가 자신의 데이터를 통합적으로 조회하고 관리할 수 있는 서비스를 제공하기 시작했다. 마이데이터 사업은 관련 법령과 가이드라인을 기반으로 운영되고 있으며, 어느 정도 체계화되어 있는 상태이다. 초기에는 모바일 앱 중심으로 서비스가 제공되었으나, 최근에는 일반 영업점 등 오프라인 채널에서도 활용 가능하도록 서비스 범위가 확대되고 있다. 이에 따라, 이용자의 편의성과 활용성을 강화한 '마이데이터 2.0 서비스'가 새롭게 출시되었다.

참고

[마이데이터 사업] 마이데이터 개념 및 마이데이터 2.0 주요 내용

· **마이데이터 개념**: 마이데이터 사업자는 금융회사 등이 보유한 개인신용정보를 수집·종합하여, 신용정보주체(금융소비자)가 조회·열람할 수 있도록 서비스를 제공

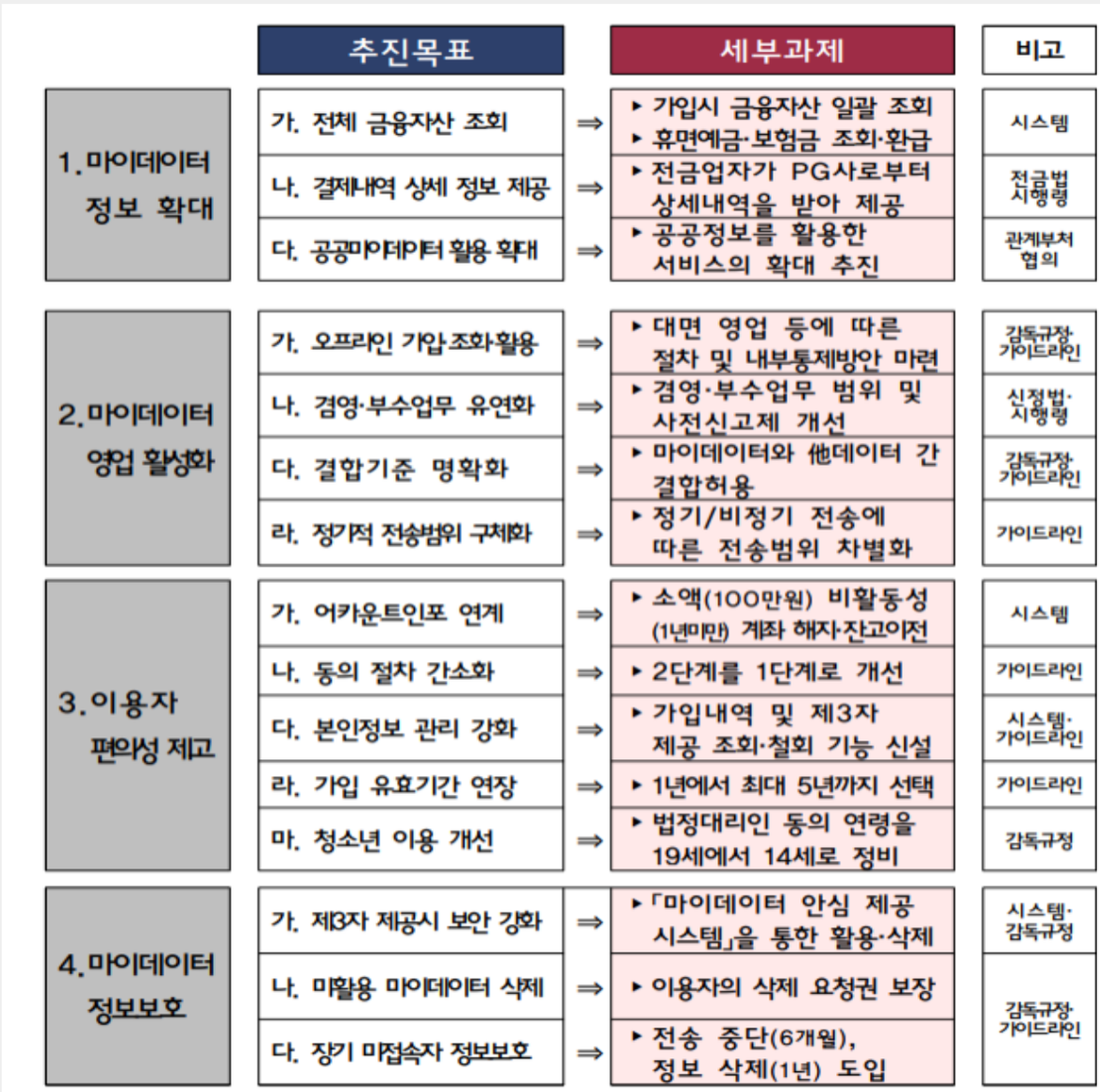
· **마이데이터 서비스 이용 절차**

① **(전송요구)** 정보주체가 정보제공자(예: 금융회사)가 보유한 자신의 신용정보를 구체적으로 지정하여 전송요구

② **(본인인증)** 정보주체는 본인인증을 통해 개별 정보제공자 또는 다수의 정보제공자에게 전송요구권 행사 가능

③ **(정보전송)** 정보제공자는 기존의 스크래핑 방식이 아닌 사전에 정해진 방식에 따라 마이데이터 사업자에게 정보전송

· **마이데이터 2.0 추진 방안**: 금융플랫폼으로서의 기능 강화를 위해 ①마이데이터 정보 확대, ②영업 활성화, ③이용자 편의성 제고, ④마이데이터 정보보호 추진



	추진목표		세부과제	비고
1. 마이데이터 정보 확대	가. 전체 금융자산 조회	⇒	▸ 가입시 금융자산 일괄 조회 ▸ 휴면예금·보험금 조회·환급	시스템
	나. 결제내역 상세 정보 제공	⇒	▸ 전금업자가 PG사로부터 상세내역을 받아 제공	전금법 시행령
	다. 공공마이데이터 활용 확대	⇒	▸ 공공정보를 활용한 서비스의 확대 추진	관계부처 협의
2. 마이데이터 영업 활성화	가. 오프라인 가입·조회·활용	⇒	▸ 대면 영업 등에 따른 절차 및 내부통제방안 마련	감독규정·가이드라인
	나. 겸영·부수업무 유연화	⇒	▸ 겸영·부수업무 범위 및 사전신고제 개선	신정법·시행령
	다. 결합기준 명확화	⇒	▸ 마이데이터와 他데이터 간 결합허용	감독규정·가이드라인
	라. 정기적 전송범위 구체화	⇒	▸ 정기/비정기 전송에 따른 전송범위 차별화	가이드라인
3. 이용자 편의성 제고	가. 어카운트인포 연계	⇒	▸ 소액(100만원) 비활동성(1년미만) 계좌 해지·잔고이전	시스템
	나. 동의 절차 간소화	⇒	▸ 2단계를 1단계로 개선	가이드라인
	다. 본인정보 관리 강화	⇒	▸ 가입내역 및 제3자 제공 조회·철회 기능 신설	시스템·가이드라인
	라. 가입 유효기간 연장	⇒	▸ 1년에서 최대 5년까지 선택	가이드라인
	마. 청소년 이용 개선	⇒	▸ 법정대리인 동의 연령을 19세에서 14세로 정비	감독규정
4. 마이데이터 정보보호	가. 제3자 제공시 보안 강화	⇒	▸「마이데이터 안심 제공 시스템」을 통한 활용·삭제	시스템·감독규정
	나. 미활용 마이데이터 삭제	⇒	▸ 이용자의 삭제 요청권 보장	감독규정·가이드라인
	다. 장기 미접속자 정보보호	⇒	▸ 전송 중단(6개월), 정보 삭제(1년) 도입	

· **마이데이터 2.0 서비스 개시('25. 6.)**: 「마이데이터 2.0 추진방안」('24.4월) 중 전체 금융자산 조회, 어카운트인포 연계, 본인정보 관리 강화, 동의절차 간소화, 정기적 전송주기 구체화 등 7개 개선사항을 반영하여 서비스 개시

* 출처: 금융위원회, 「마이데이터 2.0 추진 방안」
금융위원회(www.fsc.go.kr), 보도자료 '마이데이터가 더 편리한 내 손안의 금융 비서로 거듭납니다 - 「마이데이터 2.0」 서비스 개시'

최근 잇따른 개인정보 유출 사고와 코로나19의 영향으로 개인정보보호 및 정보보호의 중요성이 기업 경영과 직결된 핵심 요소임이 명확히 드러났다. 이에 따라, 최고경영진을 포함한 C-레벨 임원진의 관심과 지원이 확대되고 있다. 또한, 개인정보를 단순히 '보호'하는 영역을 넘어 개인정보 비식별화, 합성 데이터 생성 등 활용 중심의 정책과 산업 구조로 변화하면서 **개인정보보호산업의 영역이 지속적으로 확대**되고 있다.

이러한 환경 변화에 따라, 개인정보보호 담당자의 업무 범위와 난이도는 과거에 비해 크게 증가하였으나, 그 책임에 상응하는 법적 제도 지원, 권한, 인센티브 체계는 충분히 마련되지 못한 실정이다. 따라서 기업 및 데이터 처리 규모에 따라 전담 인력을 적정 수준으로 확보하고 업무 환경을 개선할 수 있는 제도적 장치 마련이 필요하다.

또한, '**데이터 안심구역 서비스***'를 통해 데이터를 제공하고 있는 등 해당 서비스에 대한 수요가 높지는 않은 상황이나, 향후 금융회사나 공공기관에서 신용정보, 복지 데이터 등을 활용한 예측 서비스 등 활용도가 높아질 것으로 전망된다.

참고

[데이터 안심구역 서비스] 주요 내용

- **데이터 안심구역 개념**: 데이터안심구역은 누구든지 데이터를 안전하게 분석·활용할 수 있는 구역으로서, 기술적·물리적·관리적 보안대책 등이 갖추어진 건물 또는 그 밖의 시설(가상 공간 포함)
  * 근거법령: 「데이터 산업진흥 및 이용촉진에 관한 기본법」 제11조 및 같은 법 시행령 제12조·제13조
- **데이터 안심구역 기능**: 다양한 미개방데이터의 분석을 위한 안전한 분석환경을 제공하고, 분석 시스템 및 도구, 분석 결과 반출 등을 지원
- **이용대상**: 데이터안심구역 이용 신청 후 승인을 받으면 누구나 이용 가능

* 출처: 데이터안심구역(dsz.kdata.or.kr)

더불어, 「**개인정보 보호법 시행령**」 **개정***에 따라 개인정보 처리자에 대한 기준이 보건의료, 통신, 에너지 관련 기관·법인·단체로 명확히 고지되었으며, 외부 개인정보 전송 요구 시 제공 의무가 발생함으로써 데이터 관리와 법적 준수의 중요성이 더욱 강화되고 있다.

참고

[「개인정보 보호법 시행령」] 주요 개정 사항 비교

제35조의2(개인정보의 전송 요구) [시행 2025. 3. 13.]	제42조의2(정보전송자 기준) [시행 2025. 10. 2.]
② 정보주체는 매출액, 개인정보의 보유 규모, 개인정보 처리 능력, 산업별 특성 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 대하여 제1항에 따른 전송 요구 대상인 개인정보를 기술적으로 허용되는 합리적인 범위에서 다음 각 호의 자에게 전송할 것을 요구할 수 있다. 1. 제35조의3제1항에 따른 개인정보관리 전문기관 2. 제29조에 따른 안전조치의무를 이행하고 대통령령으로 정하는 시설 및 기술 기준을 충족하는 자 ③ 개인정보처리자는 제1항 및 제2항에 따른 전송 요구를 받은 경우에는 시간, 비용, 기술적으로 허용되는 합리적인 범위에서 해당 정보를 컴퓨터 등 정보처리장치로 처리 가능한 형태로 전송하여야 한다. ④ 제1항 및 제2항에 따른 전송 요구를 받은 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 법률의 관련 규정에도 불구하고 정보주체에 관한 개인정보를 전송하여야 한다. 1.「국세기본법」 제81조의13 2.「지방세기본법」 제86조 3. 그 밖에 제1호 및 제2호와 유사한 규정으로서 대통령령으로 정하는 법률의 규정	법 제35조의2제1항 각 호 외의 부분 및 제2항 각 호 외의 부분에서 “대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 각각 다음 각 호의 어느 하나에 해당하는 자(이하 “정보전송자”라 한다)를 말한다. 1. 보건의료 관련 기관, 법인 및 단체 중 다음 각 목의 어느 하나에 해당하는 자(이하 “보건의료정보전송자”라 한다) 가. 질병관리청 나.「국민건강보험법」 제13조에 따른 국민건강보험공단 및 같은 법 제62조에 따른 건강보험심사평가원 다.「의료법」 제3조의4에 따른 상급종합병원 라. 그 밖에「보건의료기본법」 제3조제4호에 따른 보건의료기관 중 개인정보를 전송할 수 있는 기술적·재정적 능력과 그 개인정보가 저장·관리되고 있는 정보주체의 수 등을 고려하여 보호위원회가 보건복지부장관과 협의하여 고시하는 자 2. 통신 관련 기관, 법인 및 단체 중 다음 각 목의 어느 하나에 해당하는 자(이하 “통신정보전송자”라 한다) 가.「전파법」 제10조에 따라 주파수를 할당받아 이동통신서비스를 제공하는 자로서 정보주체와 이동통신서비스의 이용에 관한 계약을 체결한 자 나. 그 밖에「전기통신사업법」 제5조제2항에 따른 기간통신사업을 경영하는 자 중 개인정보를 전송할 수 있는 기술적·재정적 능력과 그 개인정보가 저장·관리되고 있는 정보주체의 수 등을 고려하여 보호위원회와 과학기술정보통신부장관이 공동으로 정하여 고시하는 자 3. 에너지 관련 기관, 법인 및 단체 중 다음 각 목의 어느 하나에 해당하는 자(이하 “에너지정보전송자”라 한다) 가.「전기사업법」 제2조제10호에 따른 전기판매사업자 나. 다음의 어느 하나에 해당하는 자 중 개인정보를 전송할 수 있는 기술적·재정적 능력과 그 개인정보가 저장·관리되고 있는 정보주체의 수 등을 고려하여 보호위원회와 산업통상부장관이 공동으로 정하여 고시하는 자 1)「도시가스사업법」 제2조제2호에 따른 도시가스사업자 2) 그 밖의「도시가스사업법」 제2조제1호의2에 따른 도시가스사업 관련 기관, 법인 및 단체

* 출처: 국가법령정보센터(www.law.go.kr)

필요 역량 및 인력 수요

개인정보 이동활용관리 직무 중 마이데이터 관련 업무는 주로 금융권에서 운영되고 있어, 해당 업무를 수행하기 위해서는 **은행 및 금융 산업에 대한 이해**가 필수적이다. 이를 위해 자산관리, 데이터 분석 등 금융업의 특성을 이해하고, 개인신용정보 처리에 필요한 접근 통제, 암호화, 금융 실명 거래와 비밀 보장, 「금융지주회사법」 등 금융권 특화 법령 및 가이드라인에 대한 지식이 요구된다.

또한, **데이터와 마이데이터 서비스에 대한 이해**도 중요하다. 마이데이터 서비스 제작 과정에서는 데이터를 분석하고 활용할 수 있어야 하며, 일부 기업에서는 자체적인 개인정보보호 시스템을 개발하기 때문에 **개발 역량**도 요구된다. 기업 규모에 따라 데이터 분석은 별도의 부서에서 수행되기도 한다.

더불어, 기본적으로 개인정보보호 담당자로서 **법령 이해 및 리스크 관리 능력**도 갖추어야 한다. 「개인정보 보호법」, 「신용정보법」, 「정보통신망」법 등 기본적인 정보보호 및 개인정보보호 관련 거버넌스와 컴플라이언스를 숙지하고, 이를 바탕으로 사업 추진과정에서 발생할 수 있는 리스크를 평가하고 관리할 수 있는 능력이 필요하다.

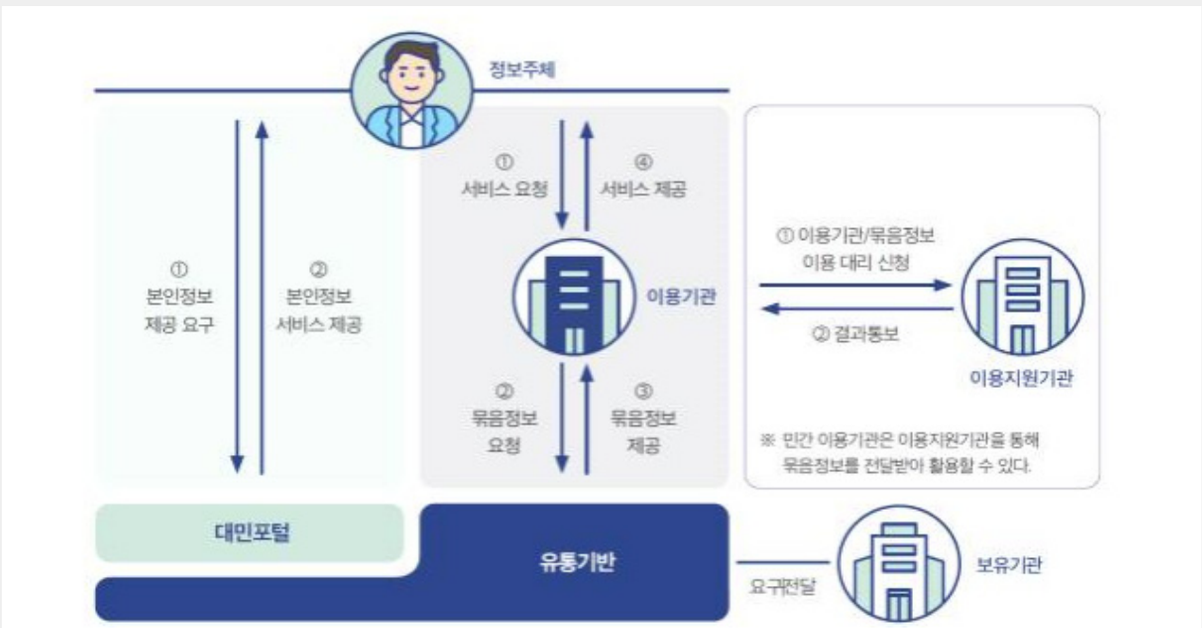
개인정보 활용과 관련해서는 가명·익명처리 기술에 대한 이해가 필요하며, 접속 기록 관리, 접근 제어, 시스템 설정 등 기술적 이해와 함께, 최근에는 AI 관련 지식도 습득해야 한다. 실무적으로는 개인정보 수집·이용 동의서, 개인정보 처리 방침 등의 문서 작성 및 활용 가이드, 내부 보안성 검토, 매뉴얼 안내 등 사업 부서에 자문을 제공하기도 한다. 따라서, 담당자는 **법, 기술, 기업 내부 프로세스를 종합적으로 숙지**해야 한다.

최근에는 **공공 마이데이터 사업***과 관련하여 행정안전부 등 공공기관에서 보관하는 등본, 가족관계증명서 등의 행정서류를 사내 시스템과 연동하여 필요한 정보를 제공하는 사례가 늘어나고 있으며, 외부 데이터 공개 요청 시 개인정보를 식별 불가능한 수준으로 가명처리하여 제공하는 업무가 요구되고 있다. 이처럼 데이터 활용과 공개가 증가하면서 정보 공개와 공공 데이터 활성화를 위한 조직이 신설되고 추가 인력 수요가 발생하고 있으며, 기술적 보호 조치와 시스템 운영을 포함한 관리·운영이 복합적으로 요구된다.

참고

[공공 마이데이터 사업] 주요 개념

- **공공 마이데이터**: 행정·공공기관 등이 보유하고 있는 정보주체의 본인정보 또는 본인정보를 적극적, 능동적으로 관리하고 활용할 수 있는 새로운 데이터 활용 체계를 의미
- **공공 마이데이터 서비스**: 정보주체의 행정정보를 가지고 있는 기관이 정보주체의 '①제공요구'에 따라 정보주체 본인 또는 정보주체가 지정한 제3자에게 '②본인에 관한 행정정보(본인정보)'를 제공하는 서비스
  * 법적근거: 「전자정부법」 제43조의2



* 출처: 행정안전부, 「공공 마이데이터 서비스 수행 가이드」

개인정보 이동활용관리 직무 수행을 위해 CPPG 자격 소지자를 우대하며, 신입은 일반 IT 관련 전공자를 채용한 후 전문 교육을 통해 업무에 배치한다. 입사 이후에도 담당자의 역량 강화를 위해 정보보안기사, 개인정보 관리사, 데이터 분석 전문가 등의 자격증 취득 지원과 내부 교육이 진행되며, 전사 차원의 개인정보보호 교육과 지사·지역 사업소 순회 교육도 진행된다. 기업 규모에 따라서는 대학과 연계하여 정보보호·개인정보보호 특화 석사 과정 등을 운영하기도 하며, 임직원의 전문성 향상을 위한 지속적인 교육을 지원하고 있다.

데이터 활용 관련 업무를 담당하는 개인정보보호 전문 인력의 수요는 꾸준히 증가하고 있다. 그러나 개인정보보호 담당자가 모든 법령을 이해하고 적용하기에는 한계가 있으므로, 변호사 등 전문 분야 계약직 인력을 채용하는 사례도 있다.

또한, 이동활용관리 직무는 일반 기업에서는 수요가 다소 낮지만, 금융권, 의료, 결합전문기관 등 특정 산업에서는 별도의 부서를 운영하고 있어 전문 인력이 지속적으로 필요한 상황이다.

개인정보 인증·평가

○ 산업 및 직무 변화

개인정보 유출 사고가 지속적으로 발생하고 ESG 경영의 중요성이 강화되면서 일반 소비자의 인식이 변화되고 있으며, 이에 따라 개인정보보호가 **기업의 핵심 리스크 관리 요소이자 신뢰 형성의 기반**으로 자리 잡고 있다.

이러한 환경 변화 속에서 개인정보보호 직무 전반에 대한 요구는 기존의 법·제도 중심에서 개인정보 처리 시스템의 기술적 보호조치, 가명 정보 처리, 데이터 품질 관리 등 보다 **세부적이고 전문화된 영역까지 확대**되는 추세이다. 더불어, 개인정보보호 업무 종사자 수가 증가하고 관련 교육과 실무경험이 축적되면서 담당자들의 **법적·기술적 전문성 또한 과거에 비해 크게 향상**되고 있다.

조직 유형별로는 공공기관과 민간기업 간에 **개인정보보호 접근 방식**에서 뚜렷한 차이가 존재한다. 공공기관은 법적 요구사항을 충족하는지 여부에 집중하는 경향이 강하며, 규정 준수 중심의 아직까지는 다소 보수적인 운영 체계를 유지하고 있다. 반면, 민간기업은 경쟁력 확보와 서비스 품질 향상을 위해 보다 기술적이고 심화된 전문 역량을 요구하는 경우가 많다.

특히, 민간에서는 담당자의 역량 강화를 위해 외부 교육, 전문 자격 취득 지원, 직무 학습 기회 제공 등 다양한 투자를 적극적으로 추진하고 있다. 이에 비해 공공기관은 예산 제약 및 제도적 한계로 인해 이러한 교육·지원 체계를 충분히 갖추기 어려운 경우가 많아, 전문성 강화의 기회가 상대적으로 부족한 상황이다.

○ 필요 역량 및 인력 수요

개인정보 인증·평가 직무는 개인정보보호 체계와 관련된 법적 요구사항과 기술적 보호조치의 적정성을 심사하는 역할을 수행하며, 단순한 적합 여부 판단을 넘어 법적 근거에 기반한 구체적인 검토와 판단이 요구된다. 따라서, 심사원은 지속적으로 **변화하는 관련 법령** 뿐 아니라 새로운 기술 환경에서 적용 가능한 **기술적 보호조치**까지도 이해하고 이를 실무에 반영해야 한다.

「개인정보 보호법」을 중심으로 「정보통신망법」, 「신용정보법」 등 관련 법령뿐 아니라 ISO/IEC 27701, 27001 등 국제 표준에 대한 이해가 필요하며, 기업의 해외 진출 시에는 GDPR 해석 능력 또한 중요한 경쟁력이 된다. 더불어, AI·클라우드 등 최신 기술 환경에서 보안·보호조치가 어떻게 구현되는지 이해하는 능력이 요구된다.

심사는 보통 3~5명 규모의 팀으로 진행되며, ISMS-P 심사의 경우 개인정보보호(P) 담당자와 정보보호(I) 담당자가 함께 구성되는 등 영역별 전문성을 조합하는 방식으로 운영된다. 심사 기간은 인증 유형과 조직 규모에 따라 간단한 경우 3일, 복합적이고 대규모인 경우 최대 7~8일이 소요된다. 또한, 심사 종료 후에는 팀장 및 팀원 간 상호 평가를 수행하여 심사의 품질을 관리하는 프로세스도 포함된다. 이 과정에서 다양한 내부 이해관계자들과 협력하여 문제를 조율·설득할 수 있는 **커뮤니케이션 능력**도 중요한 요소로 평가된다.

무엇보다 **인증심사원 자격증*은 필수 요건**으로 간주되며, **다년간의 실무 경력**이 요구되는 등 진입장벽이 존재하여 개인정보보호가 아닌 일반 보안 또는 IT 경력만으로는 해당 직무에 진입하기 어려운 특성이 있다.

참고

[인증심사원 자격증] 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증심사원 주요 내용

· **응시자격기준**

- **응시요건**: 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 13조 및 별표4에 의거 다음의 인증심사원 자격 신청 요건(①~③)을 모두 충족하여야 함
  ① 4년제 대학졸업 이상 또는 이와 동등학력을 취득한 자
  ② 정보보호 및 개인정보보호 경력을 각 1년 이상 필수로 보유
  ③ 정보보호, 개인정보보호 또는 정보기술 경력을 합하여 6년 이상을 보유
- **경력대체요건:** 다음의 학위 또는 자격을 취득한 경우 정보보호 또는 개인정보보호 또는 정보기술 경력을 대체할 수 있으며 중복으로 인정하지 않음

구분	경력인정요건	인정기간
정보보호경력	· "정보보호" 관련 박사 학위 취득자	2년
	· "정보보호" 관련 석사 학위 취득자 · 정보보안기사 · 정보시스템감사통제협회(ISACA)의 정보시스템감사사(CISA) · 국제정보시스템보안자격협회(ISC)² 의 정보시스템보호전문가(CISSP)	1년

구분	경력인정요건	인정기간
개인정보보호경력	· "개인정보보호" 관련 박사 학위 취득자	2년
	· "개인정보보호" 관련 석사 학위 취득자 · 개인정보 영향평가에 관한 고시 제6조에 따른 개인정보 영향평가 전문인력 · 개인정보관리사(CPPG)	1년
정보기술경력	· "정보기술" 관련 박사 학위 취득자 · 정보관리기술사, 컴퓨터시스템응용기술사 · 정보시스템감리사	2년
	· "정보기술" 관련 석사 학위 취득자 · 정보시스템감리원 · 정보처리기사, 전자계산기조직응용기사	1년

· **자격검정 세부내용**

출제범위	검정내용
· ISMS-P 인증기준 · (개인)정보보호 관련 법규 · (개인)정보보호 이론 및 기술 · 개인정보 생명주기	· 문제유형: 객관식 5지선다 ※ 단순질의, 복합응용, 상황판단 · 문항수: 50문항 · 시험시간: 2시간 · 관련 법규의 범위: 자격검정시 인용·제시되는 법·시행령·고시 등 관련법규는 응시자의혼란을 피하기 위하여 자격검정의 공고일 기준 시행된 법령으로 출제

* 출처: 차세대 ISMS-P 디지털 플랫폼 (isms-p.or.kr)

또한, 조직에서는 심사원의 **전문성 강화**를 위해 외부 실무 중심 교육, 세미나, 워크숍 참여를 적극 권장하고 있으며, 내부적으로는 심사 결과 사례, 통제 항목 해설, 구현 사례 분석 등 실무 기반 지식을 공유하는 구조를 강화하고 있다. 국내에서는 공공기관 주도의 다양한 교육 프로그램이 운영되고 있으며, 단순 기초 지식 전달보다는 실제 사고 분석, 법령 해석, 다각적 관점의 **사례 기반 교육에 대한 수요**가 점차 높아지고 있는 추세이다.

개인정보보호 인력에 대한 수요는 지속적인 증가세를 보이고 있으나, 컨설팅 경험을 기반으로 일반 기업의 보안 담당자로 이직하는 사례도 있어 인력 이탈이 일정 부분 발생하고 있어 이에 대한 대응도 필요해 보인다.

나. 직무구분 검토

1) 직무 세부내용 재정립

개인정보 가명·익명처리

개인정보 가명·익명처리 직무 수행 과정에서 AI와 LLM의 활용 증가로 세부 업무의 재정비가 필요한 상황이다. 특히, AI 및 LLM 기반의 **자동화와 상용 솔루션의 확산**으로 인해 별도의 전문가가 아니더라도 일정 교육을 받은 유관 부서 구성원이 업무를 수행할 수 있는 환경이 조성되는 등 업무의 범위가 조정되는 추세이다. 다만, 정부부처, 통신 등 일부 분야에서는 여전히 데이터 결합 과정에서 솔루션의 처리 가능 범위를 넘어서는 다양한 경우의 수가 발생하고 있기 때문에 수작업 기반 업무 수행 인력에 대한 수요는 유지될 것으로 보인다.

또한, 데이터 활용 환경 변화에 따라 일부 직무 담당자의의 역할도 변화하고 있다. 가명·익명처리 직무의 경우, 가명·익명처리 기획이나 위험관리보다는 가명·익명처리에 대한 적정성을 검토하고 서비스 부서에 자문하는 형태로 변화하고 있다.

개인정보보호 관리

개인정보보호 관리 직무에서는 규제 대응, 법률 분석, 정책 수립, 보호조치 기획 등의 역할 비중이 점차 확대될 것으로 생각된다. 특히, AI 서비스 도입이 가속화되면서 개인 데이터를 수집·모델링·학습하는 과정 전반을 관리하는 'AI 기반 데이터 관리' 역할이 개인정보보호 관리 분야의 핵심 업무로 추가될 것으로 예상된다. 또한, '25년 12월 개인정보보호위원회에서는 CPO 지정 신고제 도입 및 CPO에 대한 권한 강화 계획을 발표하였다. 이에 따라, 개인정보보호 책임자의 관리 역할 및 업무 범위에 대한 재정립도 필요해 보인다.

개인정보보호 운영

개인정보보호 운영 업무 중 '개인정보 안정성 확보 조치' 관련 업무는 별도의 직무로 분리해도 무방할 정도로 업무량이 방대하다. 또한, 최근 AI, 클라우드, 제로트러스트, 융합기술 등 신기술 도입과 관련된 업무가 증가함에 따라, 기존 운영 직무 내의 필요 역량을 재정립하거나 별도의 신규 직무로 신설되어도 좋을 것 같다. 더 나아가, 의료, 금융, 통신 등 특정 산업에 특화된 개인정보보호 운영 직무의 교육·훈련 모듈 개발도 필요해지고 있다.

개인정보보호 컨설팅

「개인정보 보호법」 개정에 따라, 개인정보 영향평가의 범위가 확대되면서 컨설팅 직무의 수행 범위도 점차 확대되고 있다. 특히, 평가 대상이 확대되어 공공과 민간기업에서 각각 요구하는 기술적 보호조치에 대한 이해가 필요하며, 특정 산업에서 요구하는 다양한 법령에 대한 이해가 필요하다. 또한, 신기술의 발전에 따라 AI 관련 요소가 평가항목에 추가되고 있어 이와 관련한 컨설팅 직무의 세부역량 재정립이 필요하다.

개인정보 이동활용관리

개인정보 이동활용관리 직무에서 '마이데이터' 분야는 사용자의 데이터 이동권과 자기결정권 등을 포함하는 영역으로, 개인정보 활용 서비스 기획 품질관리와는 다른 역량을 요구한다. 이에 따라 "개인정보 활용/서비스 운영"이라는 넓은 직무 범주 내에서 마이데이터 운영, 서비스 기획, 품질관리, 데이터 플랫폼 운영 등 세부 역할로 구분해도 좋을 것 같다. 특히, 서비스 기획 단계에서 데이터 이동 경로와 관리 방안을 함께 설계해야 하므로 서비스 기획 직무와 겸업하는 사례가 늘어나고 있다.

또한, 개인정보 이동활용관리 직무는 기업, 개인, 고객 등 매우 넓은 범위의 데이터 활용과 관리를 담당한다. 따라서, 마이데이터나 데이터 안심구역으로 한정하는 것이 아닌, '개인정보 데이터 관리'로의 명칭 변경을 검토할 필요가 있다.

개인정보 인증·평가

개인정보 인증·평가 직무 중 '인증'은 주로 ISMS-P를 기반으로 조직의 보호체계를 종합적으로 심사하는 역할인 반면, '평가'는 개인정보 영향평가를 중심으로 특정 서비스나 시스템의 위험요소를 분석하고 개선 방안을 도출하는 업무이다. 두 영역은 방법론, 요구 역량, 작업 흐름 모두 다르기 때문에 별도의 전문 직무로 구분하는 것이 바람직하다.

2) 직무 신설

최근 개인정보보호 분야에서는 **신기술과 관련된 직무 신설**의 필요성이 높아지고 있다. 유관 정부 부처에서도 AI, 클라우드, 딥페이크 등 신기술과 관련된 개인정보 이슈가 지속적으로 언급되고 있으며, 신기술의 확산, PbD 개념의 강화, 데이터 거버넌스 관리의 중요성 증가 등으로 인해 새로운 개인정보보호 관련 직무를 정의할 필요가 있다.

특히, **AI 활용**이 증가함에 따라 개인정보 기반 데이터셋 관리, 알고리즘 검증, AI 모델에 적용되는 기술적 보호조치 등 AI 관련 개인정보보호 직무가 새롭게 생겨났다. 또한, 정보주체의 개인정보 처리에 대한 민감성이 높아짐에 따라 개인정보의 열람 요청, 정정·삭제 요구 등 **정보주체 권리 보장** 및 대응 업무의 비중도 이전보다 크게 증가하고 있다.

이러한 신기술의 급속한 발전은 새로운 개인정보보호 직무를 필요로 하는 환경을 만들고 있으며, AI 윤리, 데이터 프라이버시 거버넌스, ESG 경영 관리 등 **신기술을 고려한 직무**가 새롭게 요구되고 있다.

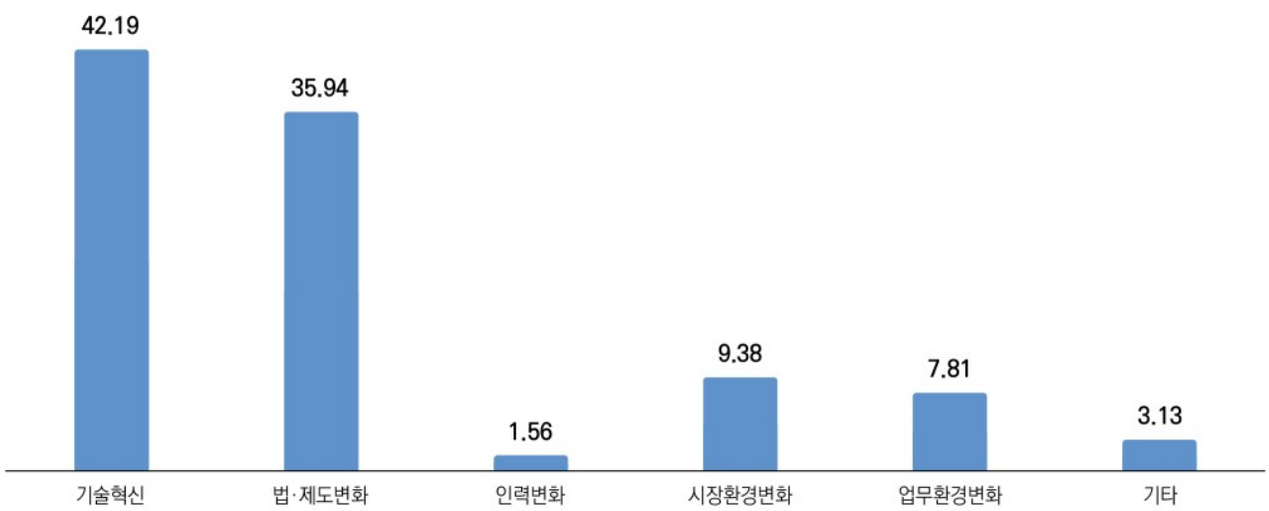
2. 산업현장 검증

가. 직무변화 선행요인

개인정보보호 산업의 직무 및 업무 과정 변화에 영향을 미치는 선행요인을 분석한 결과, 기술혁신 42.19%, 법·제도변화 35.94%, 인력변화 1.56%, 시장환경변화 9.38%, 업무환경변화 7.81%로, 기타 3.13%로 나타났다.

[개인정보보호산업 변화 선행요인]

단위: %



순위	선행요인	비중(%)
1	기술혁신(인공지능, 자동화 등)	**42.19**
2	법·제도변화	**35.94**
3	시장환경변화(시장수요, 경쟁, 등)	**9.38**
4	업무환경변화(재택근무, 스마트오피스 등)	**7.81**
5	기타	**3.13**
6	인력변화(인구감소, 처우·급여 등 개인욕구변화 등)	**1.56**

해당 응답을 선택한 이유는 다음과 같다.

연번	응답	이유
1	기술혁신	· 빅데이터, 마이데이터, AI, Web3, 양자 암호, 제로트러스트 등 다양한 신기술이 생겨남에 따라, 개인정보보호산업에 많은 변화가 생김
2		· ChatGPT 등 생성형 AI 등장 이후 AI의 활용도가 급격히 증가함에 따라, 개인정보나 권한 탈취에 AI를 활용하는 사례가 많아지고 있음
3		· 생성형 AI발전에 따른 개인정보 이용 및 유출 위험 증가
4		· 기술혁신으로 일상의 전반이 행태정보, 위치정보, SNS 등의 개인정보가 인공지능 시대에 데이터의 핵심으로 부상하였으며 이에 전세계적으로 개인정보 중요성에 대한 법제도 마련되어 준수가 요구됨
5		· 기존 개인정보보호 솔루션에 AI가 결합되면서 데이터 기반 이상탐지, 개인정보 식별 자동화, 정책추천 등 업무 난이도·방식이 변화하고 있음
6		· 개인정보보호 직무 자체가 기술 기반 설계·검증 능력을 요구하는 방향으로 변화하고 있음
7		· 디지털 혁신 및 데이터 분석을 통한 개인 맞춤형 서비스 제공 트렌드에 따라 개인정보를 좀 더 안전하게 관리해야 하는 상황임
8		· AI가 개인정보 탐지·분류·마스킹을 자동화하고 이상징후를 실시간 분석하며, 고위험 처리의 사전 대응 체계까지 지원하면서 기존의 수작업 중심 업무가 데이터 기반·지능형 프로세스로 전환되고 있음
9	법·제도변화	· 개인정보 유출 사고 발생에 따라 기업들에 대한 개인정보보호 규제가 강화되었으며, 사내의 개인정보보호 기능의 강화와 컨설팅 사업이 강화될 것으로 예상됨
10		· 정부의 법령이나 가이드라인에 따라 기업에서는 개인정보보호에 대한 사내 내규 등을 더욱 강하게 수립함
11		· 개인정보보호법, 전자금융감독규정, ISMS-P, ISO27701 등 국내외 제도 개정 주기가 빨라지고 있음
12		· 기업의 보안의 경우 비용으로 인식하는 경우가 많기 때문에, 대부분 법에 의해 강제할 때 관련 보안 투자가 집중적으로 발생되고, 필수라는 인식으로 더 관심도 갖게 되는 부분이 존재함
13		· 개인정보 관련 법률의 지속적인 개정으로 개인정보의 전문성을 갖기 위해서는 법에 대한 지식이 지속적으로 확보되어야 함
14		· 개인정보보호법, 전자금융거래법, 인공지능기본법 등 규제가 크게 변하고 있으며 이에 맞춰서 개인정보보호 직무에 기대하는 업무형태나 성격 또한 변화함
15	인력변화	· 개인정보보호 중요성이 높아지고 개인정보에 대한 사람들의 인식이 변화함
16	시장환경변화	· 대기업뿐 아니라 중견·스타트업까지 개인정보보호 전문인력 수요가 빠르게 증가하면서 시장 경쟁 환경이 변화하고 있음
17		· 개인정보 유출 사고 증가, 금융권·공공기관의 강화된 규제 등으로 컨설팅·심사 시장 규모 확대, 동시에 품질 경쟁 심화가 이뤄지고 있음

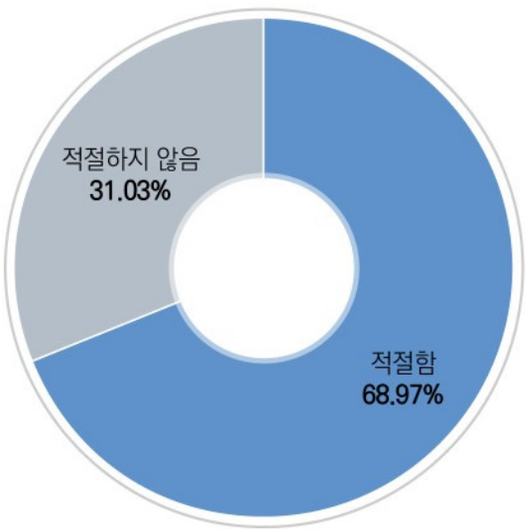
연번	응답	이유
18		· 사용자가 운영 중인 실제 컨설팅 사업에서도 고도화된 전문성 요구, 경쟁 견적 증가, 역량 기반 차별화 필요성이 커짐
19		· 최근 해킹 사고 및 잦은 개인정보 유출사고 등에 따라 변화가 예상됨
20		· 다양한 산업에서의 개인정보보호에 대한 요구수준 변화
21	업무환경변화	· 재택근무, 모바일오피스, 원격근무, 하이브리드근무 등 업무 다변화로 인한 다각도의 개인정보보호 필요성이 제기됨
22		· 코로나 이후 각종 업무 활용 Device가 다양화 되고 있어, 기존 개인정보 통제 방식이 변화함
23		· 근무방식 확대에 따라, 원격접근, 망분리 예외, SaaS 활용, 협업-도구 사용 증가 등 새로운 위협 모델이 증가하여 ZeroTrust 기반으로 변화하고 있음
24	기타	· 글로벌 규제 정합성 요구
25		· 글로벌 서비스 확산으로 GDPR, CCPA 등 해외 규제와의 정합성 준수 요구가 증가하여, 컨설턴트 및 심사원의 역할도 단순 국내 기준 검토에서 글로벌 법규 기반 검토로 확장되고 있음
26		· 규제기관의 점검요청 증가
27		· 담당 업무 외 대외 업무 증가(고객 민원 대응 등)

나. 직무구분의 적절성

개인정보보호 분야 직무맵을 기준으로 개인정보보호산업의 직무구분의 적절성을 분석한 결과, 적절하다는 의견의 68.97%, 적절하지 않다는 의견이 31.03%로 나타났다.

[직무구분의 적절성]

단위: %



* 5점 척도 기준으로 응답 (1 ~ 2: 적절함 / 3 ~ 5: 적절하지 않음)

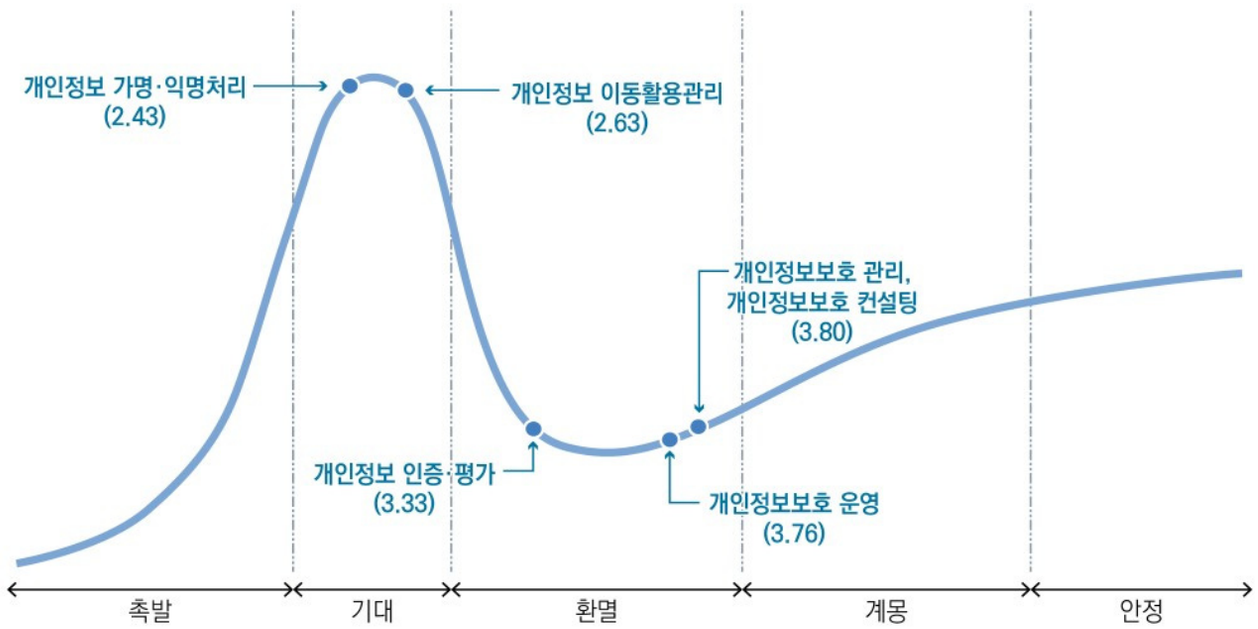
적절하지 않다고 응답한 이유로는 ▲직무 구분이 실제 산업 현황을 충분히 반영하지 못하고 있음, ▲개인정보 생명주기에 기반한 구성 기준으로 개선 필요 ▲다양한 관점의 개인정보 담당자의 업무 반영 필요 등이 있다.

한편, 기업 규모에 따라 상반된 의견도 나타났는데, 소규모 기업에서는 직무 내용이 지나치게 세분화되어 있다는 의견이 제기된 반면, 대규모 기업에서는 직무 구분이 과도하게 통합되어 있다는 의견이 도출되었다.

다. 직무별 성숙도

가트너(Gartner)의 하이프 사이클(Hype Cycle)에 기준으로 국내 개인정보보호산업의 직무별 성숙도를 5단계로 나누어 설문조사를 실시한 결과, 개인정보보호 관리(3.80), 개인정보보호 컨설팅(3.80), 개인정보보호 운영(3.76), 개인정보 인증·평가(3.33) 직무는 '환멸' 단계로, 개인정보 이동활용관리(2.63), 개인정보 가명·익명처리(2.43) 직무는 '기대' 단계로 나타났다.

[국내 개인정보보호산업 직무별 성숙도]



순위	직 무	성숙도(평균)	단계
1	개인정보보호 관리	3.80	환멸
1	개인정보보호 컨설팅	3.80	환멸
3	개인정보보호 운영	3.76	환멸
4	개인정보 인증·평가	3.33	환멸
5	개인정보 이동활용관리	2.63	기대
6	개인정보 가명·익명처리	2.43	기대

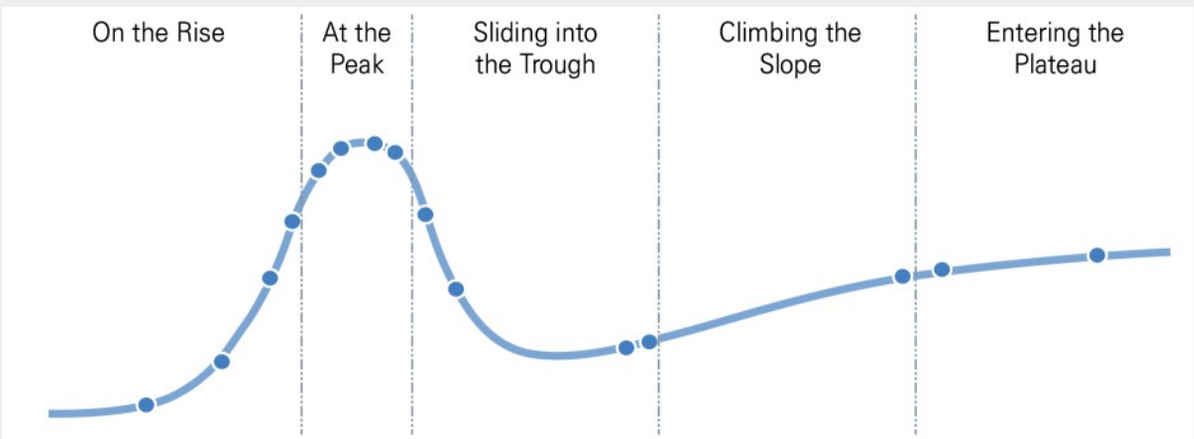
* 5점 척도 기준 (1: 촉발 / 2: 기대 / 3: 환멸 / 4: 계몽 / 5: 안정)

참고

가트너의 하이프 사이클

- 가트너(Gartner) 주식회사는 전 세계 85개국에 고객사를 두고 있는 미국의 정보 기술 연구 및 자문회사로, 시장 분석 결과의 시각화 도구로 하이프 사이클 및 매직 쿼드런트를 개발하여 사용하고 있다.
- 하이프 사이클(Hype Cycle)은 기술의 성숙도를 표현하기 위한 시각적 도구로 성장 주기에 따라 5개의 단계로 이루어진다.

[하이프 사이클 구조]



* 출처: Gartner 홈페이지(www.gartner.com/)

단계		특징
1	촉발	• 잠재적 기술이 관심을 받기 시작하는 시기이며, 초기 단계의 개념적 모델과 미디어의 관심이 대중의 관심을 불러일으킨다. • 상용화된 제품은 없고 상업적 가치도 아직 증명되지 않은 상태이다. → 해당 업무에 대한 관심이 높아지기 시작하여, 직무의 수요가 예상되는 단계
2	기대	• 초기의 대중성이 일부의 성공적 사례와 다수의 실패 사례를 양산해 낸다. • 일부 기업이 실제 사업에 착수하지만, 대부분의 기업들은 관망한다. → 해당 업무에 대한 관심이 매우 높아져, 직무 종사자가 나타나기 시작하는 단계
3	환멸	• 실험 및 구현이 결과물을 내놓지만 실패함에 따라 관심이 시들해진다. • 제품화를 시도한 주체들은 포기하거나 실패한다. • 살아남은 사업 주체들이 소비자들을 만족시킬만한 제품의 향상에 성공한 경우에만 투자가 지속된다. → 해당 업무에 대한 관심이 시들해짐에 따라, 일부 회사에서만 직무 담당자를 지정하는 단계
4	계몽	• 기술의 수익 모델을 보여 주는 좋은 사례들이 늘어나고 더 잘 이해되기 시작한다. • 2-3세대 제품들이 출시된다. • 더 많은 기업들이 사업에 투자하기 시작한다. • 보수적인 기업들은 여전히 유보적인 입장을 취한다. → 해당 업무가 인정받기 시작하여, 다수의 회사에서 직무 담당자를 보유하기 시작하는 단계
5	안정	• 기술이 시장의 주류로 자리 잡기 시작한다. • 사업자의 생존 가능성을 평가하기 위한 기준이 명확해진다. • 시장에서 성과를 거두기 시작한다. → 해당 업무가 자리 잡기 시작함에 따라, 다수의 회사에서 직무 담당자를 안정적으로 보유하는 단계

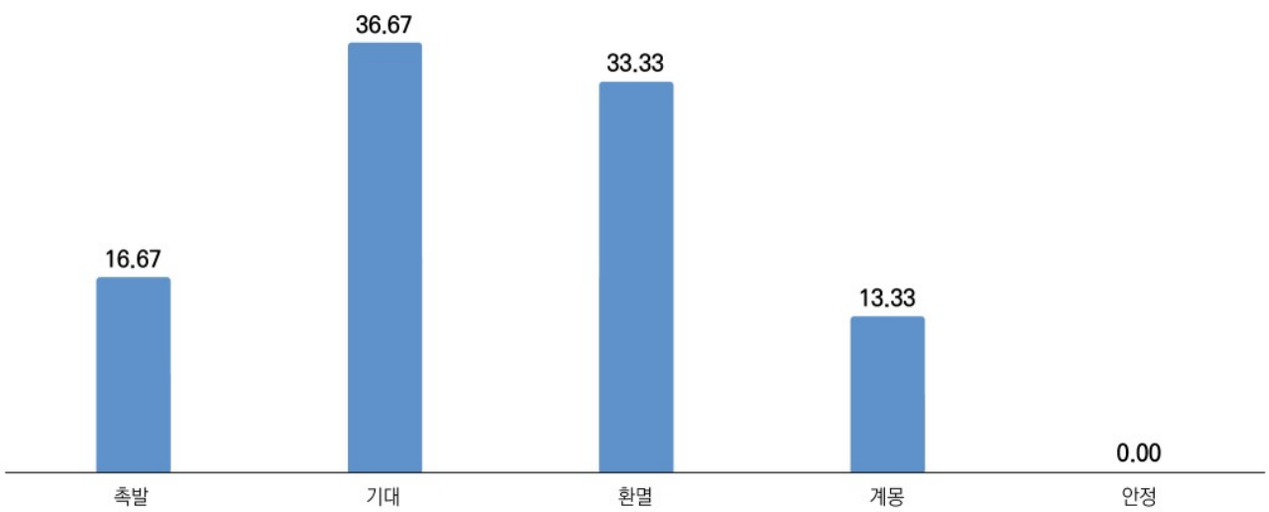
직무별 산업 내 성숙도는 다음과 같다.

개인정보 가명·익명처리

개인정보 가명·익명처리 직무의 산업 내 성숙도는 촉발 16.67%, 기대 36.67%, 환멸 33.33%, 계몽 13.33%, 안정 0.00%로 나타났다.

[개인정보 가명·익명처리 직무 산업 내 성숙도]

단위: %

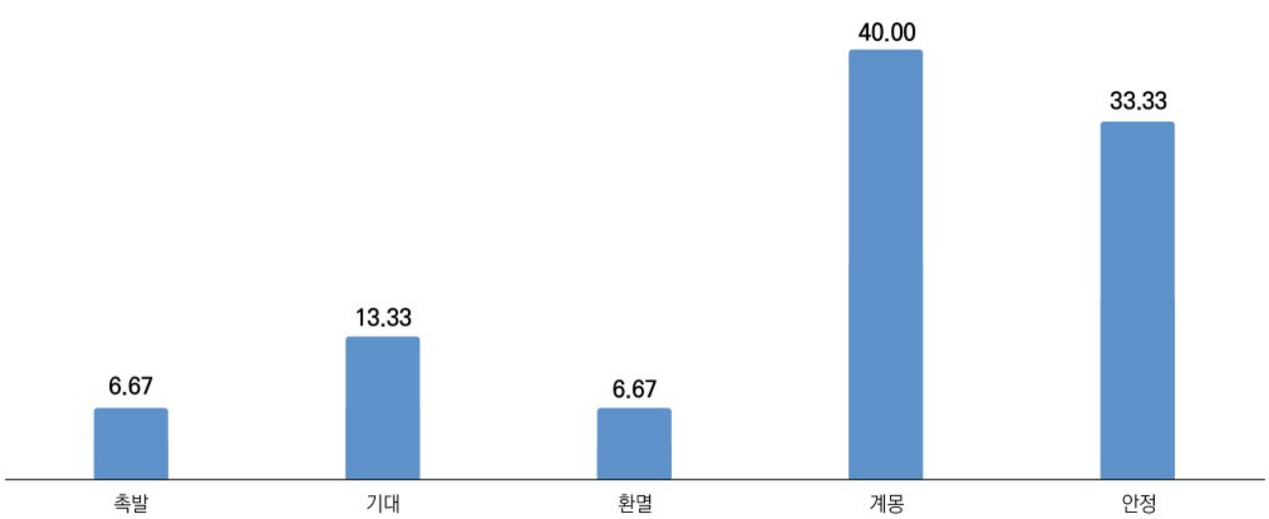


개인정보보호 관리

개인정보보호 관리 직무의 산업 내 성숙도는 촉발 6.67%, 기대 13.33%, 환멸 6.67%, 계몽 40.00%, 안정 33.33%로 나타났다.

[개인정보보호 관리 직무 산업 내 성숙도]

단위: %

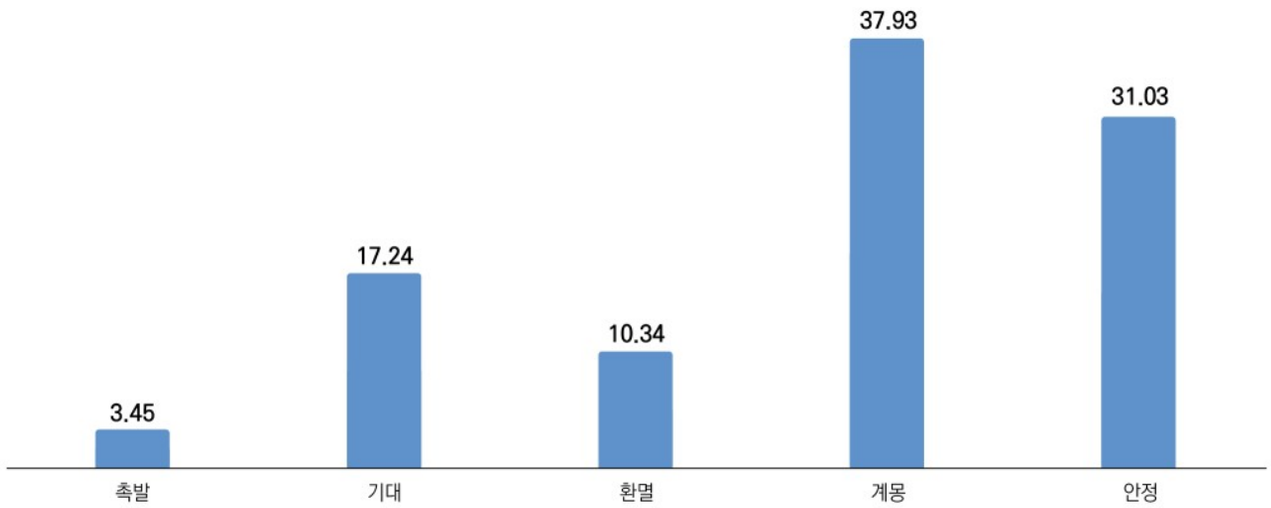


개인정보보호 운영

개인정보보호 운영 직무의 산업 내 성숙도는 촉발 3.45%, 기대 17.24%, 환멸 10.34%, 계몽 37.93%, 안정 31.03%로 나타났다.

[개인정보보호 운영 직무 산업 내 성숙도]

단위: %

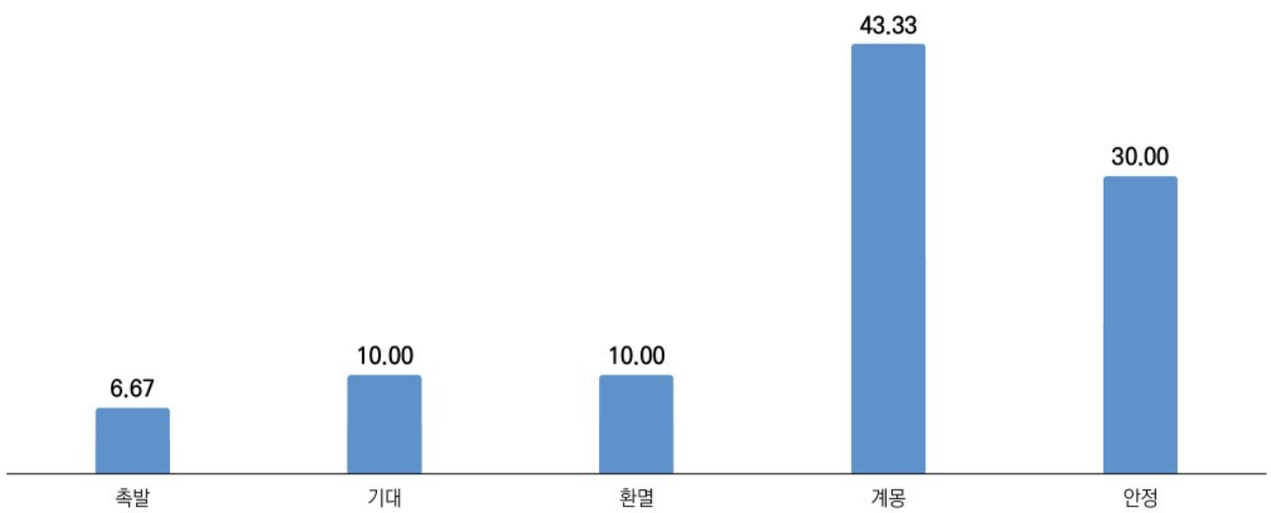


개인정보보호 컨설팅

개인정보보호 컨설팅 직무의 산업 내 성숙도는 촉발 6.67%, 기대 10.00%, 환멸 10.00%, 계몽 43.33%, 안정 30.00%로 나타났다.

[개인정보보호 컨설팅 직무 산업 내 성숙도]

단위: %

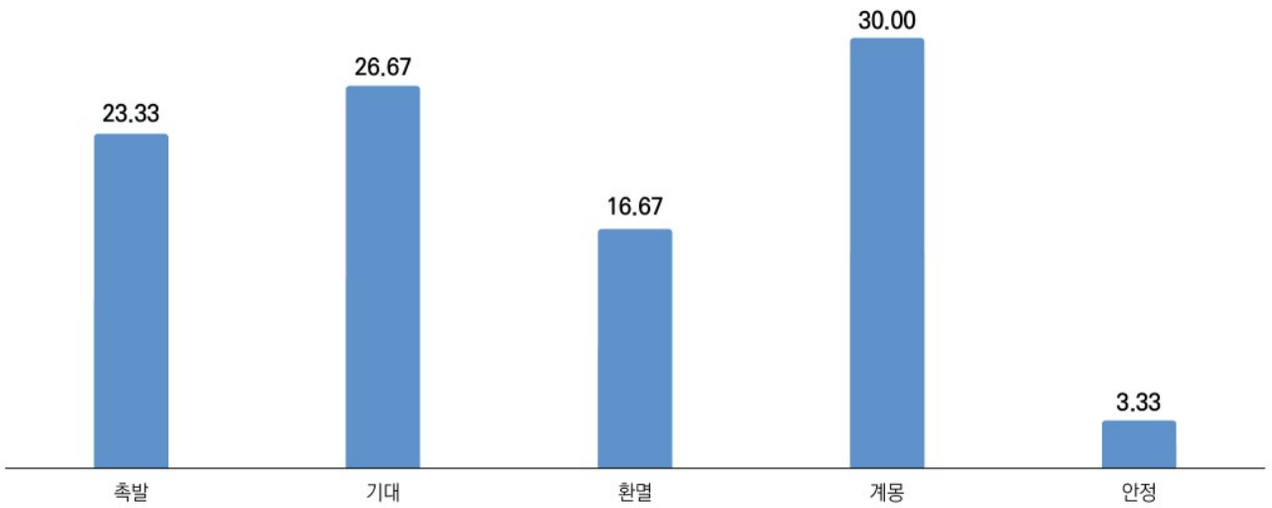


개인정보 이동활용관리

개인정보 이동활용관리 직무의 산업 내 성숙도는 촉발 23.33%, 기대 26.67%, 환멸 16.67%, 계몽 30.00%, 안정 3.33%로 나타났다.

[개인정보 이동활용관리 직무 산업 내 성숙도]

단위: %

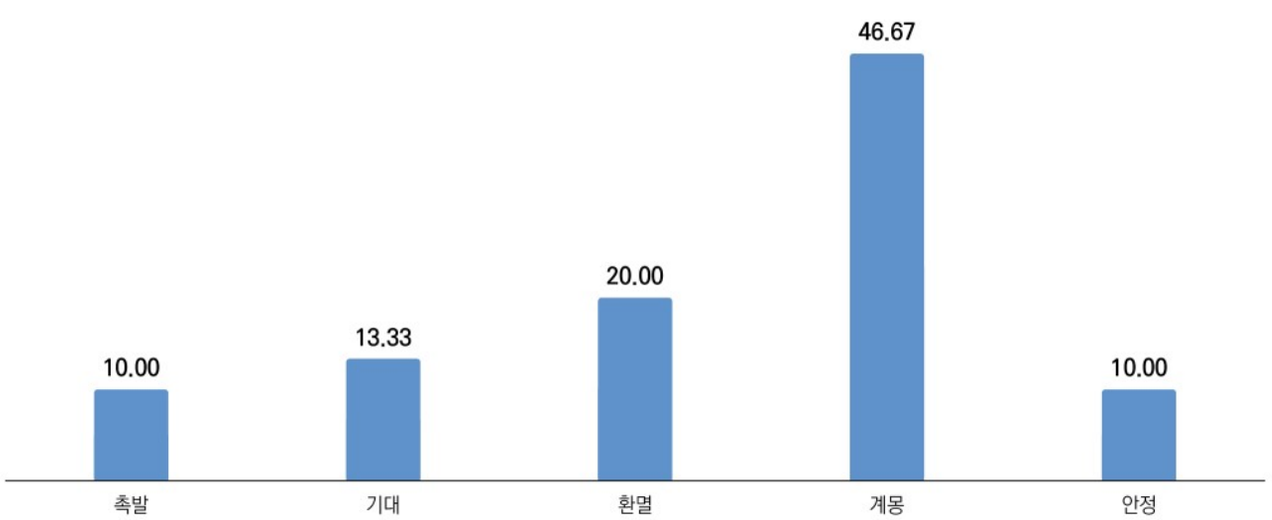


개인정보 인증·평가

개인정보 인증·평가 직무의 산업 내 성숙도는 촉발 10.00%, 기대 13.33%, 환멸 20.00%, 계몽 46.67%, 안정 10.00%로 나타났다.

[개인정보 인증·평가 직무 산업 내 성숙도]

단위: %



라. 직무수준

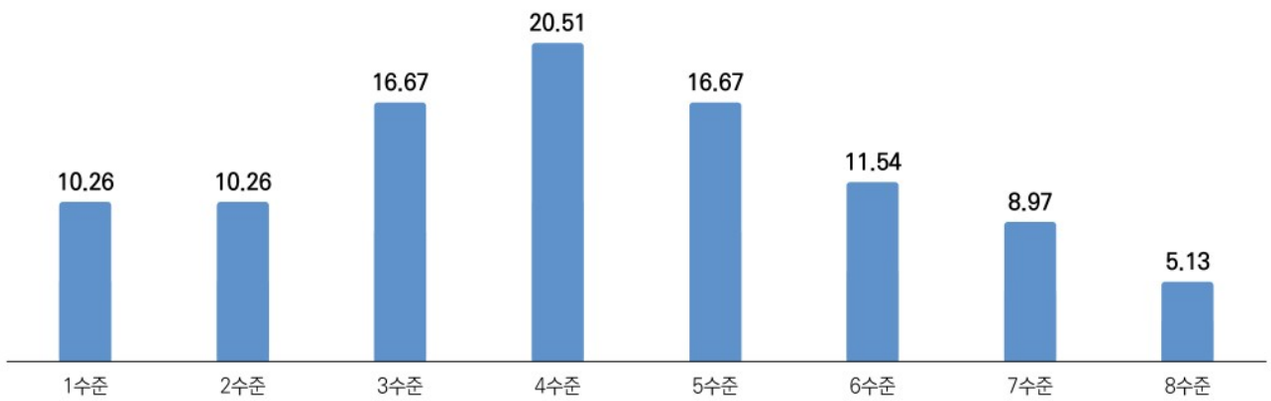
NCS에서 구분하고 있는 직무수준에 기반한 직무별 인력의 수준 분포는 다음과 같다.

○ 개인정보 가명·익명처리

개인정보 가명·익명처리 담당 인력의 직무수준은 1수준 10.26%, 2수준 10.26%, 3수준 16.67%, 4수준 20.51%, 5수준 16.67%, 6수준 11.54%, 7수준 8.97%, 8수준 5.13%로 분포된 것으로 나타났다.

[개인정보 가명·익명처리 직무수준]

단위: %

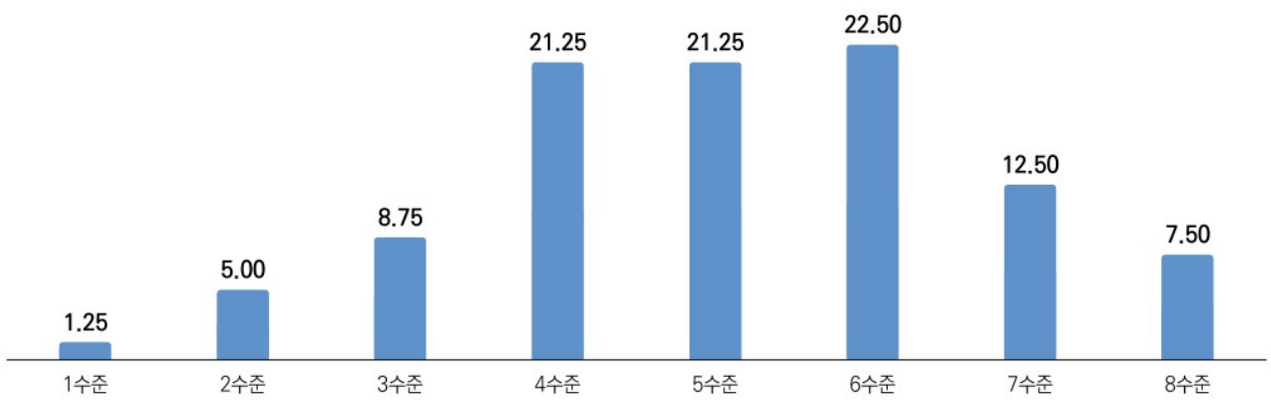


○ 개인정보보호 관리

개인정보보호 관리 담당 인력의 직무수준은 1수준 1.25%, 2수준 5.00%, 3수준 8.75%, 4수준 21.25%, 5수준 21.25%, 6수준 22.50%, 7수준 12.50%, 8수준 7.50%로 분포된 것으로 나타났다.

[개인정보보호 관리 직무수준]

단위: %

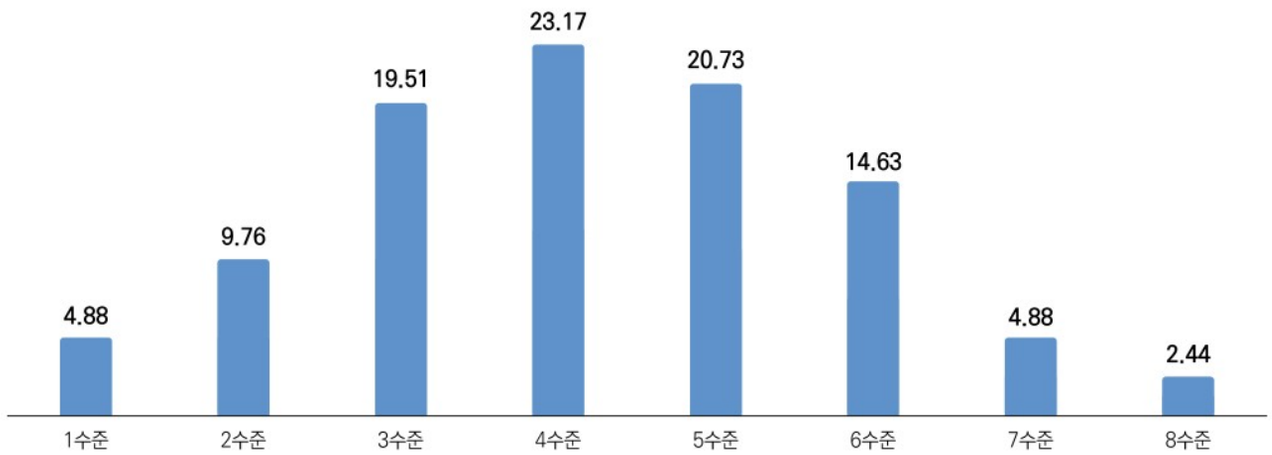


개인정보보호 운영

개인정보보호 운영 담당 인력의 직무수준은 1수준 4.88%, 2수준 9.76%, 3수준 19.51%, 4수준 23.17%, 5수준 20.73%, 6수준 14.63%, 7수준 4.88%, 8수준 2.44%로 분포된 것으로 나타났다.

[개인정보보호 운영 직무수준]

단위: %

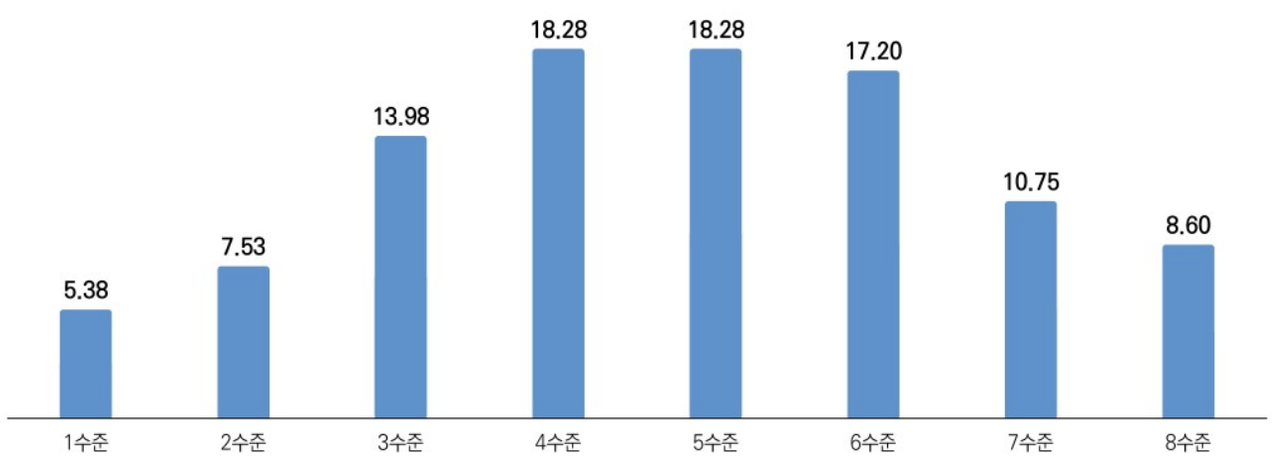


개인정보보호 컨설팅

개인정보보호 컨설팅 담당 인력의 직무수준은 1수준 5.38%, 2수준 7.53%, 3수준 13.98%, 4수준 18.28%, 5수준 18.28%, 6수준 17.20%, 7수준 10.75%, 8수준 8.60%로 분포된 것으로 나타났다.

[개인정보보호 컨설팅 직무수준]

단위: %

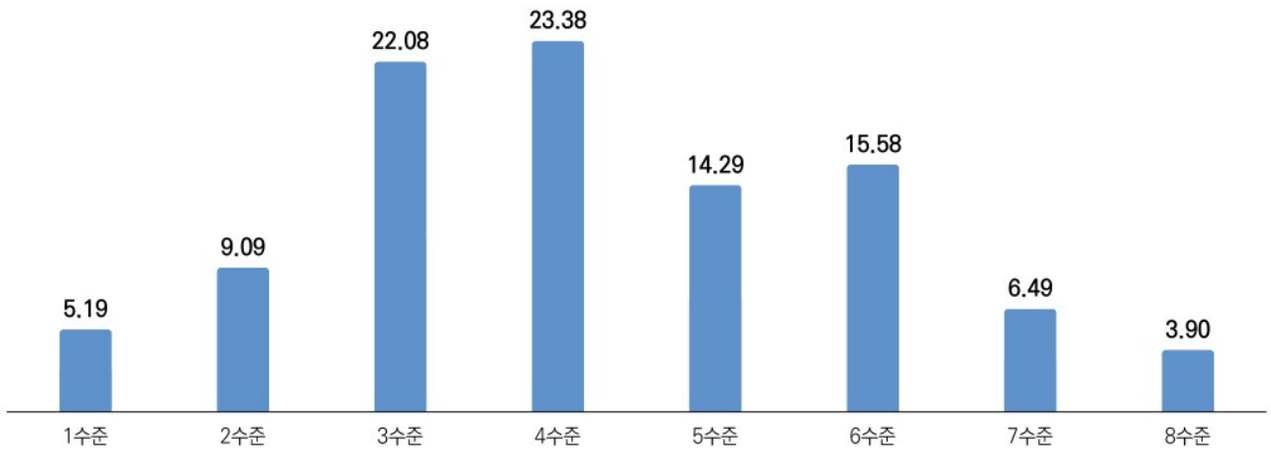


개인정보 이동활용관리

개인정보 이동활용관리 담당 인력의 직무수준은 1수준 5.19%, 2수준 9.09%, 3수준 22.08%, 4수준 23.38%, 5수준 14.29%, 6수준 15.58%, 7수준 6.49%, 8수준 3.90%로 분포된 것으로 나타났다.

[개인정보 이동활용관리 직무수준]

단위: %

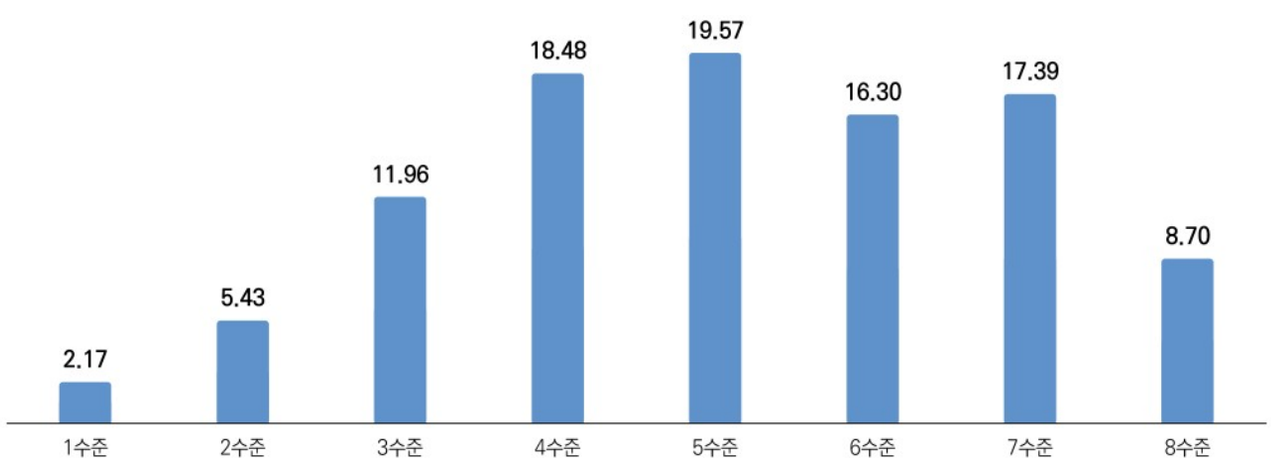


개인정보 인증·평가

개인정보 인증·평가 담당 인력의 직무수준은 1수준 2.17%, 2수준 5.43%, 3수준 11.96%, 4수준 18.48%, 5수준 19.57%, 6수준 16.30%, 7수준 17.39%, 8수준 8.70%로 분포된 것으로 나타났다.

[개인정보 인증·평가 직무수준]

단위: %



마. 직무변화

개인정보보호 분야의 직무별 변화도를 분석한 결과, 개인정보보호 관리와 개인정보보호 인증·평가 직무가 각각 3.20으로 가장 높은 변화를 보였다. 그 외 개인정보 이동활용관리(3.13), 개인정보보호 운영(3.07), 개인정보보호 컨설팅(3.00), 개인정보 가명·익명 처리(2.87) 순으로 나타났다.

순위	직 무	변화도(평균)
1	개인정보보호 관리	3.20
1	개인정보 인증·평가	3.20
3	개인정보 이동활용관리	3.13
4	개인정보보호 운영	3.07
5	개인정보보호 컨설팅	3.00
6	개인정보 가명·익명처리	2.87

* 5점 척도 기준으로 응답 (1: 전혀 달라지지 않음 ~ 5: 완전히 달라짐)

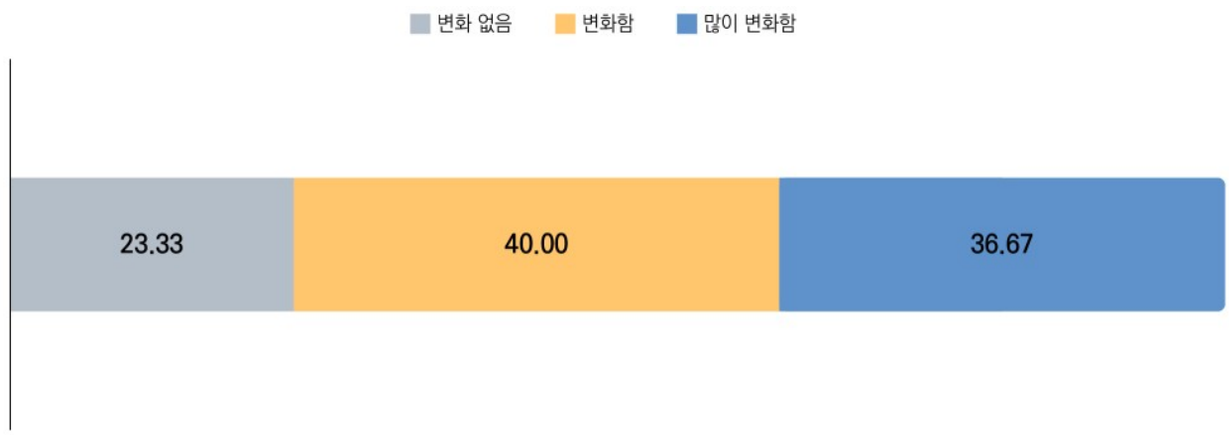
직무별 변화 정도 및 요인은 다음과 같다.

개인정보 가명·익명처리

개인정보 가명·익명처리 직무의 직무변화 정도는 변화없음 23.33%, 변화함 40.00%, 많이 변화함 36.67%로 나타났다.

[개인정보 가명·익명처리 직무변화 정도]

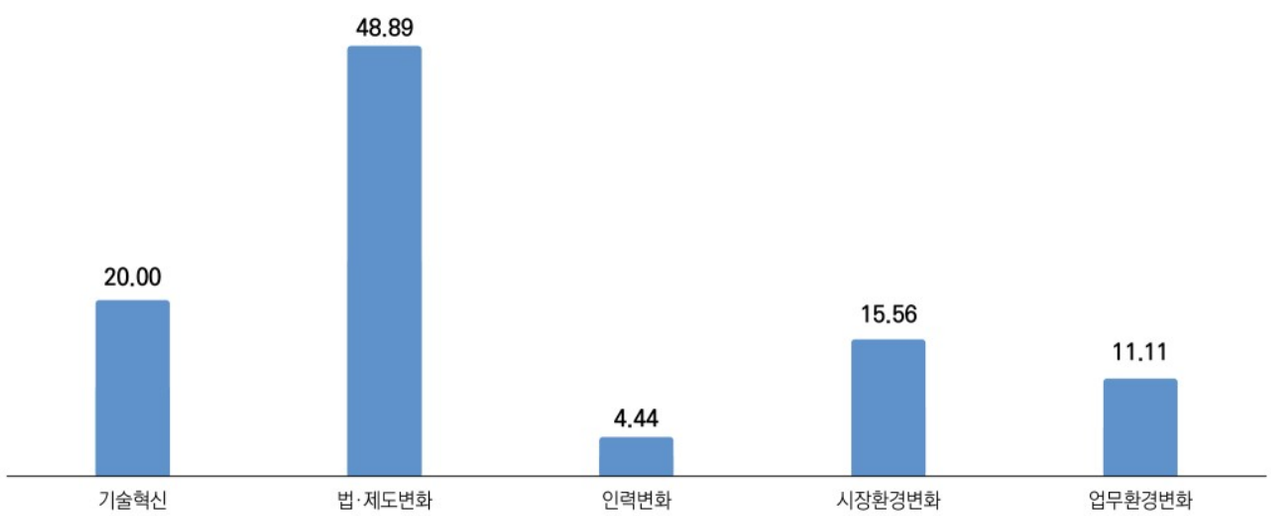
단위: %



개인정보 가명·익명처리 직무의 주요 변화요인은 기술혁신 20.00%, 법·제도변화 48.89%, 인력변화 4.44%, 시장환경변화 15.56%, 업무환경변화 11.11%로 나타났다.

[개인정보 가명·익명처리 직무변화요인(복수 응답)]

단위: %

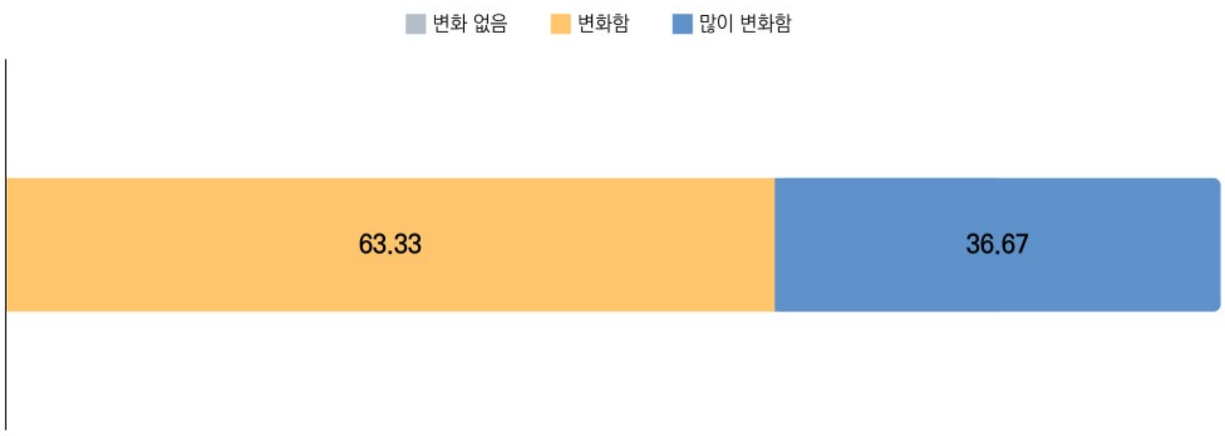


개인정보보호 관리

개인정보보호 관리 직무의 직무변화 정도는 변화없음 0.00%, 변화함 63.33%, 많이 변화함 36.67%로 나타났다.

[개인정보보호 관리 직무변화 정도]

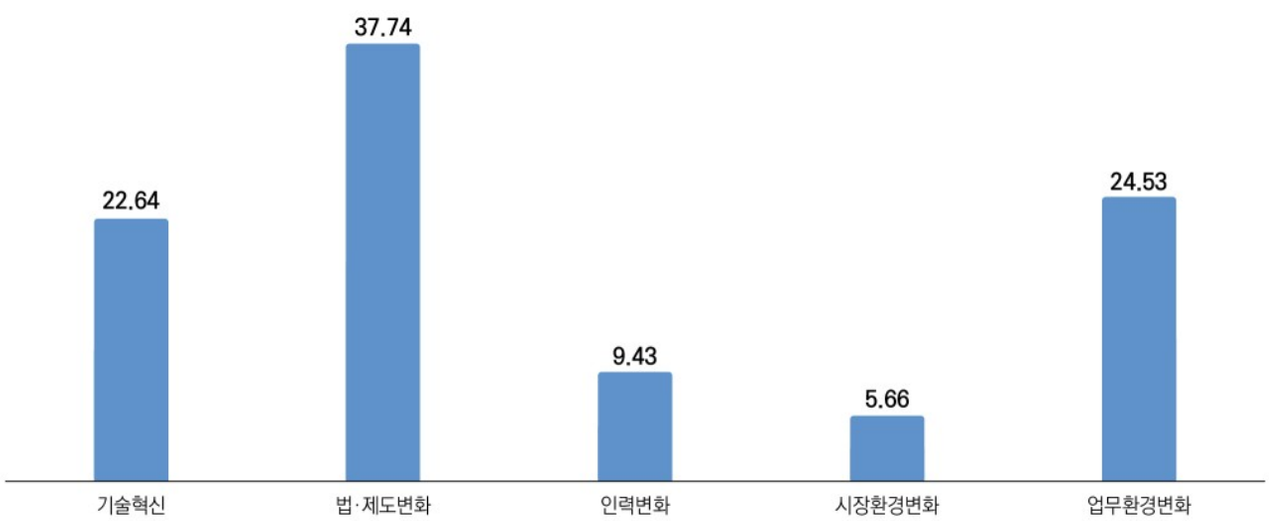
단위: %



개인정보보호 관리 직무의 주요 변화요인은 기술혁신 22.64%, 법·제도변화 37.74%, 인력변화 9.43%, 시장환경변화 5.66%, 업무환경변화 24.53%로 나타났다.

[개인정보보호 관리 직무변화요인(복수 응답)]

단위: %



개인정보보호 운영

개인정보보호 운영 직무의 직무변화 정도는 변화없음 3.33%, 변화함 70.00%, 많이 변화함 26.67%로 나타났다.

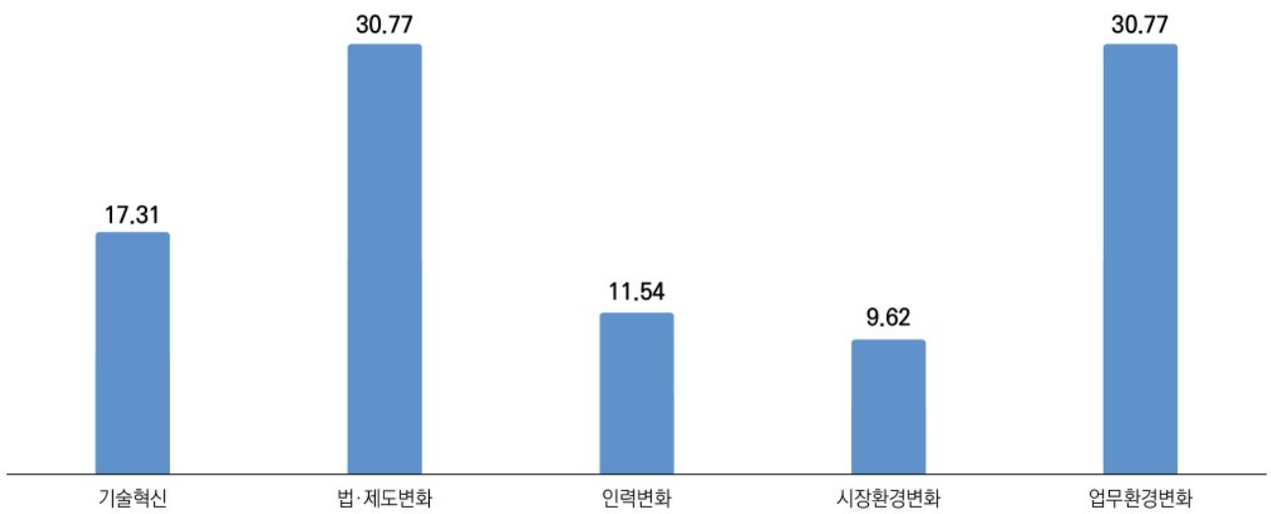
[개인정보보호 운영 직무변화 정도]

단위: %

개인정보보호 운영 직무의 주요 변화요인은 기술혁신 17.31%, 법·제도변화 30.77%, 인력변화 11.54%, 시장환경변화 9.62%, 업무환경변화 30.77%로 나타났다.

[개인정보보호 운영 직무변화요인(복수 응답)]

단위: %

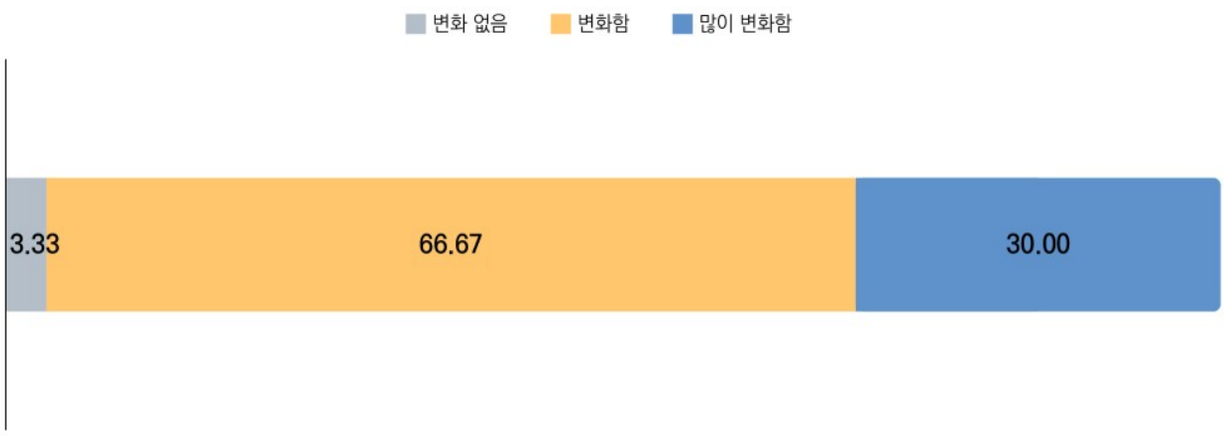


개인정보보호 컨설팅

개인정보보호 컨설팅 직무의 직무변화 정도는 변화없음 3.33%, 변화함 66.67%, 많이 변화함 30.00%로 나타났다.

[개인정보보호 컨설팅 직무변화 정도]

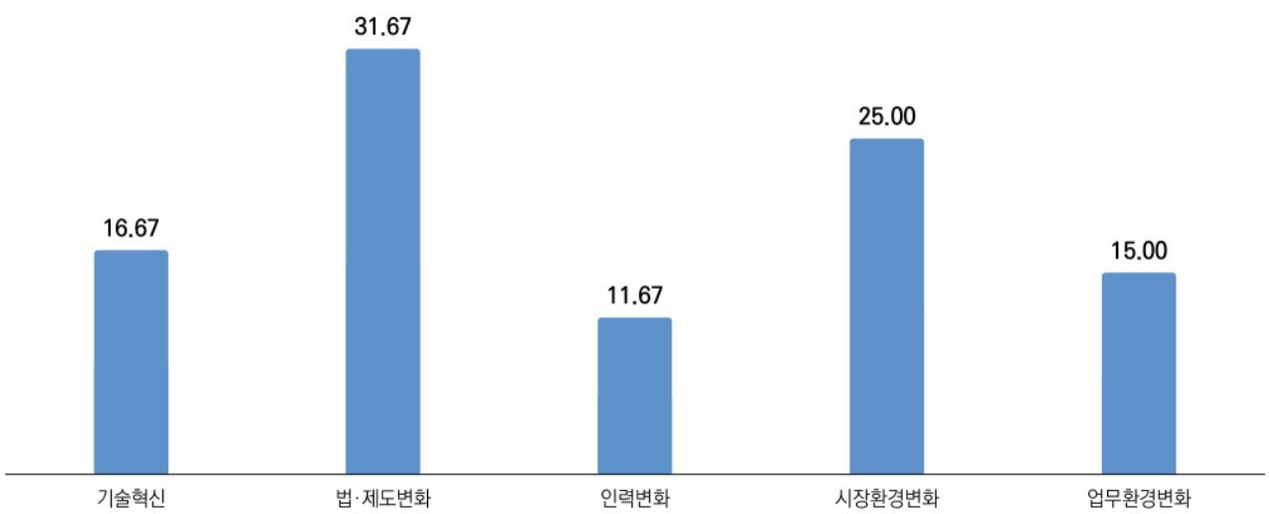
단위: %



개인정보보호 컨설팅 직무의 주요 변화요인은 기술혁신 16.67%, 법·제도변화 31.67%, 인력변화 11.67%, 시장환경변화 25.00%, 업무환경변화 15.00%로 나타났다.

[개인정보보호 컨설팅 직무변화요인(복수 응답)]

단위: %

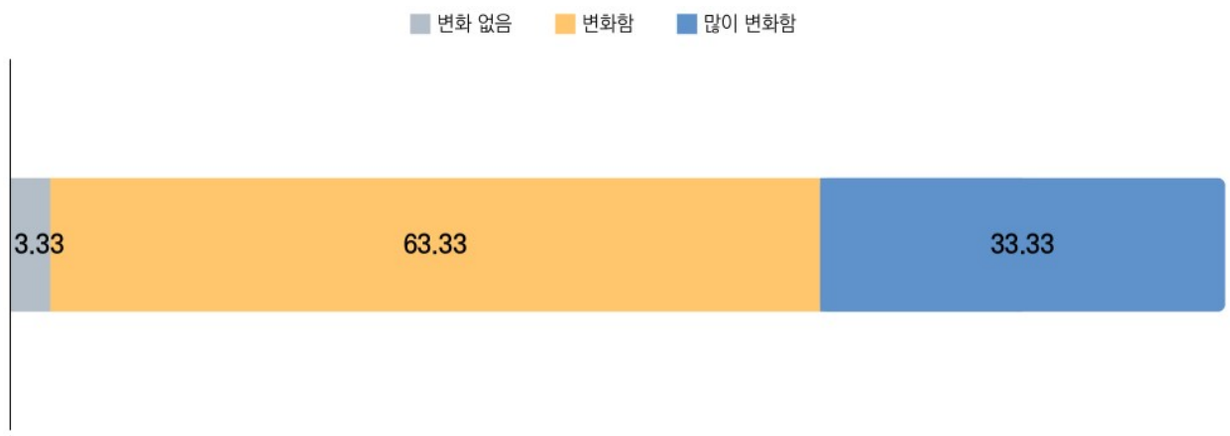


개인정보 인증·평가

개인정보 인증·평가 직무의 직무변화 정도는 변화없음 3.33%, 변화함 63.33%, 많이 변화함 33.33%로 나타났다.

[개인정보 인증·평가 직무변화 정도]

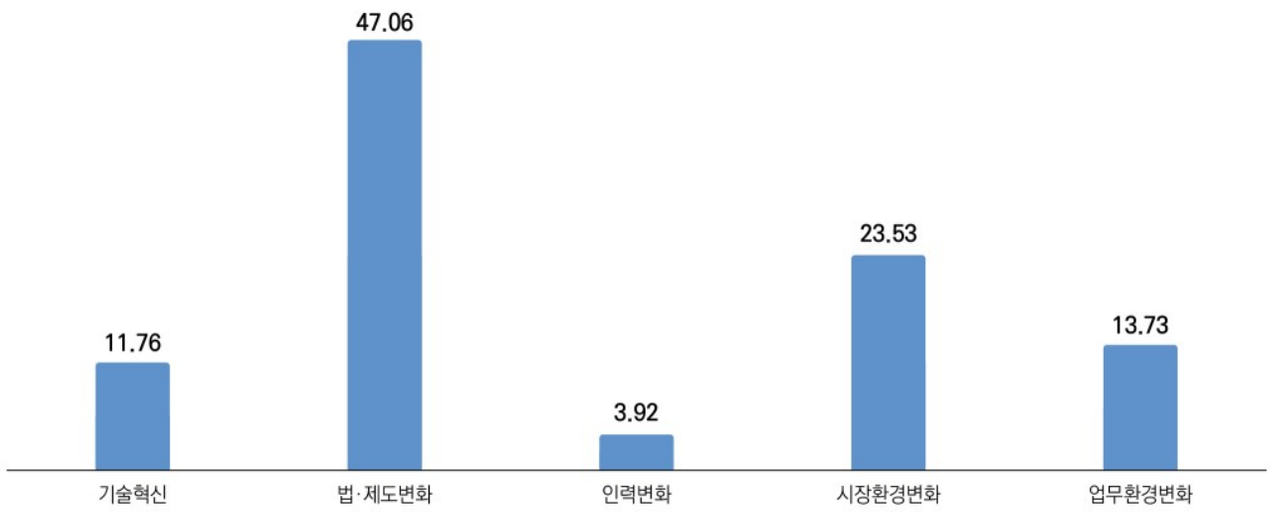
단위: %



개인정보 인증·평가 직무의 주요 변화요인은 기술혁신 11.76%, 법·제도변화 47.06%, 인력변화 3.92%, 시장환경변화 23.53%, 업무환경변화 13.73%로 나타났다.

[개인정보 인증·평가 직무변화요인(복수 응답)]

단위: %



바. 인력수요

향후 5년 이내 개인정보보호 분야 직무별 인력 수요 전망을 분석한 결과, 개인정보보호 관리와 개인정보보호 인증·평가 직무가 각각 2.27로 가장 높은 수요를 보였다. 그 외 개인정보보호 컨설팅(2.30), 개인정보 가명·익명 처리(2.47), 개인정보보호 운영(2.53), 개인정보 이동활용관리(2.67) 순으로 나타났다.

순위	직 무	인력수요(평균)
1	개인정보보호 관리	2.27
1	개인정보 인증·평가	2.27
3	개인정보보호 컨설팅	2.30
4	개인정보 가명·익명처리	2.47
5	개인정보보호 운영	2.53
6	개인정보 이동활용관리	2.67

* 5점 척도 기준으로 응답 (1: 매우 높음 ~ 5: 매우 낮음)

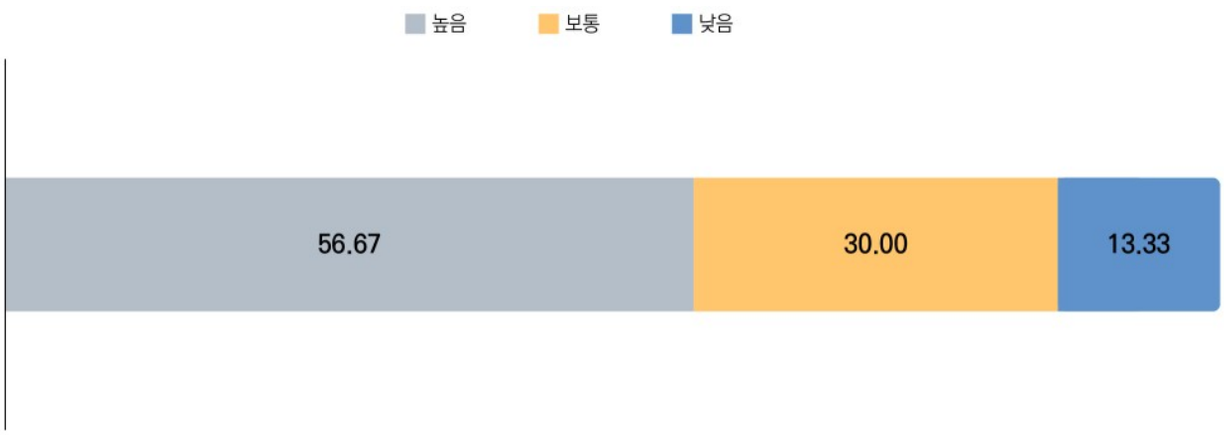
직무별 세부 인력수요는 다음과 같다.

○ 개인정보 가명·익명처리

개인정보 가명·익명처리 직무의 향후 5년간 예상 인력수요는 높음 56.67%, 보통 30.00%, 낮음 13.33%로 나타났다.

[개인정보 가명·익명처리 직무 예상 인력수요]

단위: %

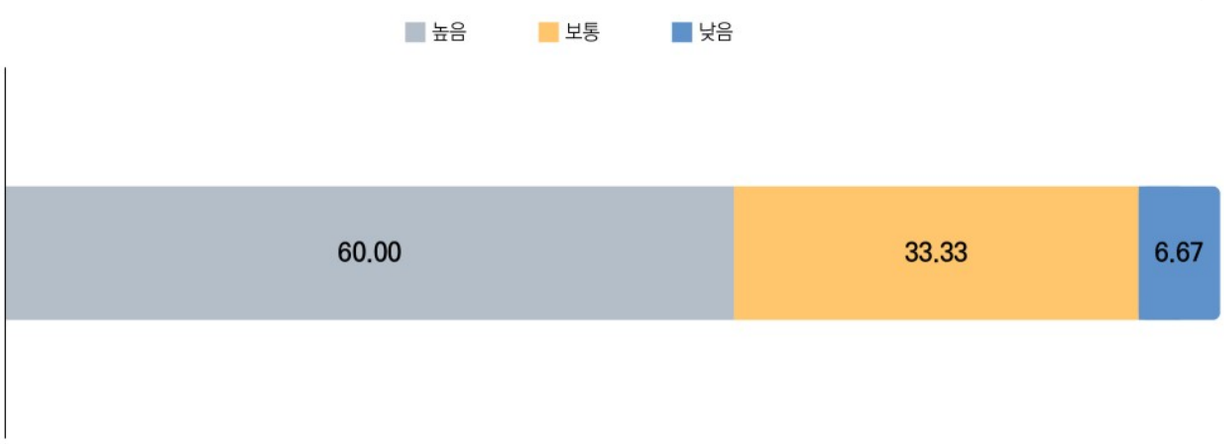


○ 개인정보보호 관리

개인정보보호 관리 직무의 향후 5년간 예상 인력수요는 높음 60.00%, 보통 33.33%, 낮음 6.67%로 나타났다.

[개인정보보호 관리 직무 예상 인력수요]

단위: %

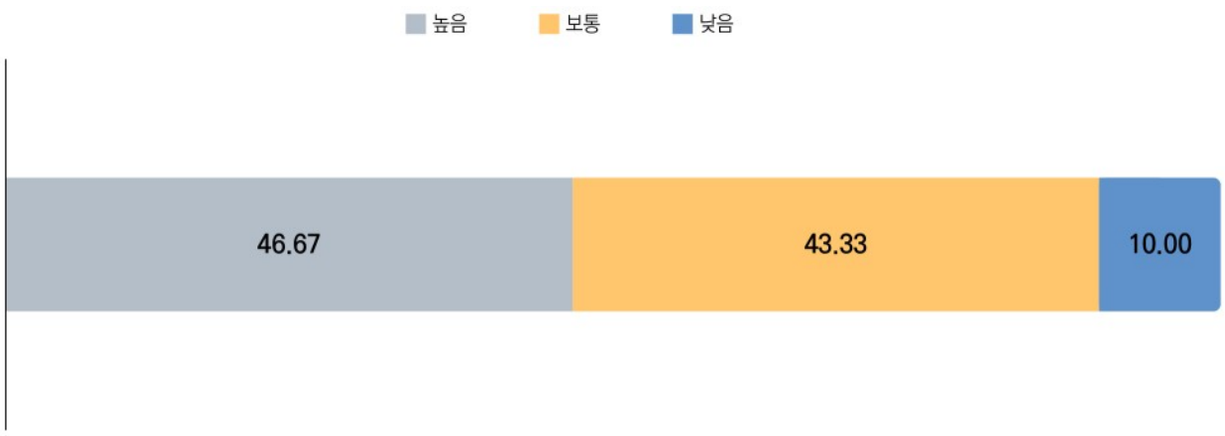


개인정보보호 운영

개인정보보호 운영 직무의 향후 5년간 예상 인력수요는 높음 46.67%, 보통 43.33%, 낮음 10.00%로 나타났다.

[개인정보보호 운영 직무 예상 인력수요]

단위: %

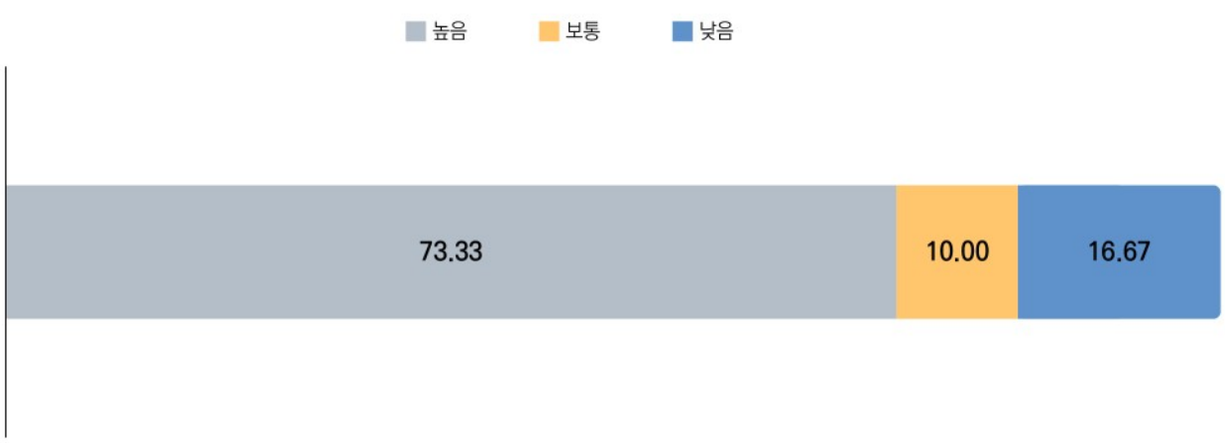


개인정보보호 컨설팅

개인정보보호 컨설팅 직무의 향후 5년간 예상 인력수요는 높음 73.33%, 보통 10.00%, 낮음 16.67%로 나타났다.

[개인정보보호 컨설팅 직무 예상 인력수요]

단위: %

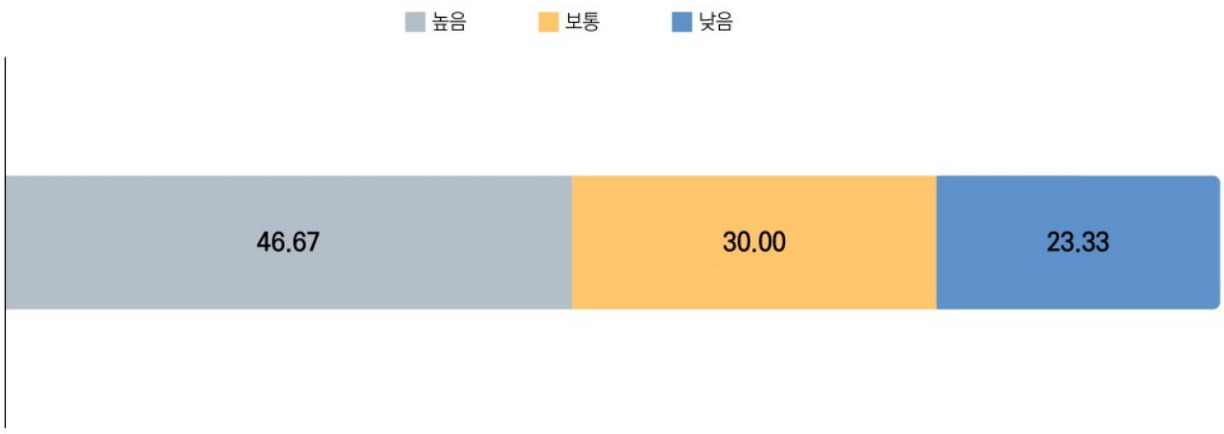


개인정보 이동활용관리

개인정보 이동활용관리 직무의 향후 5년간 예상 인력수요는 높음 46.67%, 보통 30.00%, 낮음 23.33%로 나타났다.

[개인정보 이동활용관리 직무 예상 인력수요]

단위: %

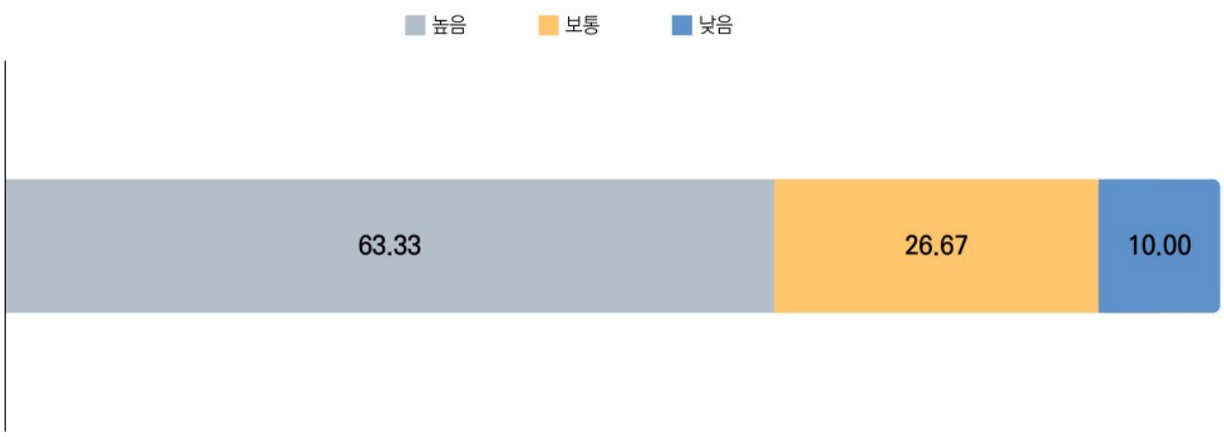


개인정보 인증·평가

개인정보 인증·평가 직무의 향후 5년간 예상 인력수요는 높음 63.33%, 보통 26.67%, 낮음 10.00%로 나타났다.

[개인정보 인증·평가 직무 예상 인력수요]

단위: %



이러한 인력수요 전망에 따라, 현재 구분된 직무 외에 새롭게 생겨난 직무(신생직무)나 사라진 직무(소멸직무), 통합·분할 등 대체되고 있는 직무(대체직무)에 대하여 다음과 같은 의견이 도출되었다.

변화양상	직무	
신생직무	인공지능(AI) 개인정보보호	· AI 개인정보 위험관리 전문가 · AI 개인정보 리스크 관리 · AI 개인정보 탐지·마스킹 운영 담당자 · AI 보안/프라이버시 규제 대응 전문가
	개인정보 위탁	· 개인정보 위탁관리 · 국내대리인 (「개인정보 보호법」 제31조의2에서 규정)
	사고 대응	· 개인정보 피해 검증 · 노출 개인정보 추적 및 제거 · 내부정보 유출 대응 담당자
	개인정보 데이터	· 데이터 이동/API 개인정보 담당자 · 개인정보 데이터 거버넌스 담당자 · 산업 맞춤형 개인정보 데이터 활용 담당자 · 데이터 프라이버시 엔지니어
	기타	· 클라우드 개인정보보호 담당자 · Zero-Trust 기반 접근제어 아키텍트 · 위치·디바이스·행동 기반의 동적 정책 설계 및 운영 · 개인영상정보처리 전문가
소멸직무	수작업 기반 작업	· 물리·수기 문서 관리 담당자 * 단, 공공기관은 사회적 취약계층의 접근성 등을 고려하여 종이문서 기반 처리를 여전히 유지함 · 수동 개인정보 점검 담당자
	단순 시스템 운영	· 단순 시스템 운영 · 단순 모니터링, 로그점검 담당자
대체직무	AI 기반 자동화	· 개인정보 가명·익명처리 → AI 기반 자동화
	업무 확장	· 개인정보보호 실무자 → 프라이버시 PM/데이터보호총괄(DPO) · 단순 준수(task) 중심 → 서비스·데이터 생명주기 관리(PM) · 보안인증(ISO·ISMS-P) 담당 → 거버넌스·리스크·컴플라이언스(GRC) 관리

사. 기타의견

이외에도 설문조사를 진행하면서 개인정보보호산업과 직무 전반에 대한 전문가들의 다양한 의견을 확인할 수 있었다.

개인정보보호산업에 대한 의견

연번	의견
1	· 개인정보보호 담당자만의 업무가 아닌, 개인정보보호 분야의 중요도가 강화되는 만큼 기술적·관리적·물리적 보호조치 등이 모두 가능한 역량을 갖춘 전문 인력 배양과 관리가 필요함
2	· 개인정보보호 관련 법규 외 전방위적 개인정보보호 지식 습득과 관련 내용을 준수할 수 있는 인력 양성이 필요하다고 판단함

직무구분 및 변화에 대한 의견

연번	의견
1	· 개인정보 유출 사고 대응 및 과징금 산정에 대한 전문성도 별도로 구분되면 좋을 것 같음
2	· 최근 정보주체 요구가 계속 증가하고 있어 이에 대한 대응이 쉽지 않음
3	· 개인정보보호 분야의 직무는 정책·거버넌스, 가명·익명처리, 개인정보 라이프사이클 운영, 영향평가·보안설계, 침해 사고 대응, 교육·모니터링 등으로 세분화되고 있음
4	· 단순히 법규 준수나 정보보안의 일부였던 개인정보보호 직무의 범위가 확대됨에 따라 개인정보보호는 전문적, 독립적, 전략적인 핵심 직무로 부상하고 있음
5	· 전체적으로 개인정보보호 직무는 기술 변화 속도에 맞춰 규제 대응, 데이터 활용, 조직 리스크 관리 역량을 동시에 요구하는 방향으로 진화하고 있음
6	· 개인정보 체계는 데이터 등급(CSO)에 따라 재편되고 있으며, 인공지능 시대에 데이터 중요도가 커짐에 따라 DB 외에 데이터웨어하우스 등에 대한 전문성이 요구되고 있음. 이러한 분산 병렬 컴퓨팅 환경에 맞는 신생 직무가 포함되면 좋을 것 같음
7	· 인공지능(AI) 도입에 따른 개인정보보호를 포함한 안전 및 관리 업무에 여러 도전이 예상됨
8	· 개인정보보호 직무는 단순 점검 중심에서 데이터 기반·위험 기반·AI 기반 체계로 고도화되고 있으며, 개인정보 자동탐지·마스킹, PIA 고도화, 권리행사 SLA 관리 등 전문성이 강화된 역할이 확대되고 있음
9	· 최근 직무변화 요인은 생성형 AI·클라우드 확산, 개인정보보호법·GDPR 등 규제 강화, 데이터 활용 시장 확대, 조직의 디지털 전환 등이 핵심으로 작용하고 있음

연번	의견
10	· 법 규제의 변화에 따라 모든 직무가 영향을 받고 있는 상황으로 기업의 컴플라이언스 준수가 매우 중요해지는 분위기임
11	· 실무자의 역량이 보안 및 컴퓨터 공학 등의 기술 이해도가 필요했다면, 앞으로는 문과나 이과 통합형 역량이 필요할 것으로 예상됨
12	· 개인정보보호 교육 전문가는 별도로 구분되어야 한다고 생각됨
13	· 영상정보와 행태정보, 위치정보 등에 대한 전문성이 포괄되면 좋을 것 같음
14	· 개인정보보호에 대한 관심이 높아짐에 따라, 최근 기업의 고객센터에 개인정보 관련 전문 상담원을 상주시키는 경우도 있음. 이처럼 개인정보 관련 민원의 수도 늘어나고 있지만, 고객 응대에 포커싱을 둔 기존 상담원들은 대응이 미흡한 경우가 많음. 따라서, 개인정보보호 관리 직무에 개인정보 민원대응을 포함해도 좋을 것 같음

2025 개인정보보호산업 직무변화 모니터링 보고서

결론 및 제언

PART. 05

5 결론 및 제언

1. 시사점

1) NCS·직무맵 내 '개인정보보호 관리' 및 '개인정보보호 운영' 직무 구분

개인정보보호 직무는 기술 발전과 데이터 활용 확대에 따라 개인정보 처리 환경이 고도화되면서 점차 세분화되고 있다. 이러한 변화로 인해 개인정보보호 정책 수립 및 내부 통제 중심의 관리 영역과, 개인정보 처리 시스템 및 기술적 보호조치의 실행·운영을 담당하는 운영 영역 간 역할과 책임의 구분이 필요해지고 있다. 이에 따라, **개인정보보호 관리 직무와 운영 직무의 구분도 명확**해지고 있다.

'개인정보보호 관리' 직무는 개인정보보호 내부관리계획 수립, 조직 정책 기획, 보호조치 체계 설계 등 전략·기획 업무를 수행한다. 세부적으로는 컴플라이언스 준수, 법령 및 정책 이해, 조직 내 개인정보보호 정책 기획, 리스크 관리, 수탁사 관리, 정보주체 권리 보장 등 관리적 보안 업무를 담당한다.

➲ **주요 키워드**: 개인정보보호 법령 분석, 개인정보보호 정책 기획, 개인정보 생명주기 관리 등

'개인정보보호 운영' 직무는 개인정보 처리 시스템 운영, 기술적 보호조치 적용 등 개인정보보호 솔루션 운영의 업무를 수행한다. 세부적으로는 개인정보 처리 시스템과 취급자의 업무 환경 운영, 기술적 보호조치 적용, 로그 관리, 비식별화 등 실무적인 시스템 및 솔루션 운영 업무를 수행한다.

➲ **주요 키워드**: 개인정보 처리시스템 운영, 개인정보 기술적 보호조치, 로그 관리, 협력사 관리 등

따라서, 현행 **직무맵** 상 '개인정보보호 관리' 직무에 구분되어 있는 '개인정보 기술적 보호조치' 등 기술 기반의 주요 업무 키워드를 '개인정보보호 운영' 직무에 포함하여 **재정립**할 필요가 있다.

또한, '개인정보보호 관리' 직무는 개인정보보호 기획, 내부 가이드 및 기준 검토, 법령 해석, 개인정보 처리 영향 분석 등 컴플라이언스 기반의 개인정보보호 정책과 절차를 총괄 관리하는 역할을 담당한다. 이에 비해 '개인정보보호 운영' 직무는 개인정보 처리 시스템

운영, 개인정보 침해·유출 사고 대응, 암호화·접근통제 등 기술적 보호조치의 적용과 운영을 중심으로 한 실무적 역할을 수행한다. 이러한 업무를 고려하여 **NCS 직무를 구분**하는 것이 필요하며, 이를 통한 직무별 역량, 교육 체계, 전문 인력 양성 체계 수립이 필요하다.

다만, 기업 규모가 작은 중소기업이나 스타트업의 경우 인력과 자원의 제약으로 인해 두 직무를 통합하여 운영하는 사례도 존재하며, 이 경우 직무 과중 및 전문성 저하를 방지하기 위한 외부 지원이나 단계적 직무 분리가 함께 고려될 필요가 있다.

2) 기업 규모 및 형태에 따른 인력 수요

개인정보보호 분야는 기업의 규모와 형태에 따라 직무 구분, 업무 범위에도 뚜렷한 차이가 나타나고 있다.

먼저, **일반 대기업**의 경우, 대부분 **개인정보보호 전담 조직**을 두고 있으며, CPO(개인정보보호책임자), 개인정보보호 기획·정책 담당, 법·컴플라이언스 전문가, 기술적 보호조치 담당자 등 **직무를 세분화하여 운영**하고 있다. 이들은 관련 법령에 대한 이해뿐 아니라 글로벌 규제 대응 역량, ISMS-P 등 인증 관리 경험, 내부 통제 및 감사 대응 능력까지 요구된다. 특히, 기업에서 영위하는 사업의 특성에 따라, 특정 **산업에 특화된 개인정보보호 역량**이 필요하기도 하다.

반면, **일반 중견·중소기업**에서는 자본 및 인력의 제약으로 인해, 전담 조직을 두기보다는 IT 관리자 또는 보안 담당자 등 타부서에서 **개인정보보호 업무를 병행**하는 형태가 다수이다. 별도의 조직이 운영된다 하더라도, 내부 관리계획 수립, 개인정보 처리 현황 관리, 침해 대응 및 외부 점검 대응 등 **개인정보보호 유관 업무가 소수의 인력에 의해 수행**되는 경우가 많다. 따라서, 개인정보보호 관련 광범위한 지식을 요구하고 있다.

또한, 일반기업의 개인정보보호 담당자가 아닌 **개인정보보호 솔루션·서비스를 운영하는 전문기업**에서는 또 다른 양상을 보인다. 전문기업은 고객사를 대상으로 컨설턴트, 인증·심사, 법·정책 자문, 개인정보보호 시스템 점검 등 다양한 개인정보보호 솔루션과 서비스를 제공하고 있다. 이에 따라, 개인정보보호산업 전반에 대한 폭넓은 이해와 함께 법·제도 분석, 기술적 능력, 커뮤니케이션 능력, 프로젝트 수행 역량이 요구되며, 실무 경험과 자격증의 중요성도 상대적으로 높다.

이러한 차이를 종합해보면, 개인정보보호산업에서의 직무와 인력에 대한 수요는 기업의 규모와 사업 구조에 따라 크게 달라진다. 따라서, 개인정보보호 직무에서는 단순히 법 지식 및 기술 역량을 쌓는 것을 넘어, **기업의 유형과 산업의 특성을 고려한 맞춤형 역량 개발 모듈이 마련될 필요**가 있다.

3) 개인정보보호 분야 교육훈련 수요

○ 사례 기반 실무 중심 교육

개인정보보호 업무는 다양한 법·제도 및 가이드라인을 기반으로 법적 요구사항을 충족하고 개인정보 유출 예방·대응을 위해, 「개인정보 보호법」을 비롯한 유관 법령과 정부 정책, 산업별 규제 등의 **변화를 지속적으로 파악하고 이에 적합한 기술적 보호조치를 적용**할 수 있어야 한다. 특히, 개인정보 처리 과정은 시스템 구축, 데이터 수집·활용, 제공, 파기, 안전성 확보 등 여러 단계로 구성되어 있어, 각 단계별 특성을 고려한 적절한 보호조치, 사고 대응 방안을 선택할 수 있는 실무적 판단 역량이 중요하다.

그러나, 실제 업무 환경에서는 이론적 지식만으로는 효과적인 대응이 어려운 상황이 빈번하게 발생한다. 기술적 문제뿐만 아니라 특정 산업에 적용되는 법령과 가이드라인, 관련 판례 등 다양한 예외 사항이 존재하기 때문에, 유사한 문제를 해결해 본 실무 경험이나 대응 전략이 매우 중요하다. 이에 따라, 단순한 법령 교육을 넘어 실제 사례를 기반으로 한 실무 중심 교육이 필수적이다.

실제로 많은 기업에서는 임직원들에게 최신 트렌드 및 정책 세미나, 워크숍, 실무 중심 교육 등의 참석을 권장하고 있으며, 사내에서도 다양한 방법론 및 수행경험을 공유하는 등 다각적 관점의 **사례 기반 교육에 대한 수요**가 점차 높아지고 있는 추세이다.

○ 개인정보 보호책임자(CPO) 체계 마련

개인정보 보호책임자(CPO) 체계 마련의 중요성도 지속적으로 강조되고 있다. 「개인정보 보호법」의 개정으로 CPO 지정 제도가 본격적으로 시행되면서, 대규모 또는 민감한 개인정보를 처리하는 개인정보처리자는 일정 수준의 전문성과 자격을 갖춘 인력을 CPO로 반드시 지정해야 한다. 하지만, 일부 기업의 경우 순환보직 등으로 인한 지속적인 경력 개발 구조가 마련되어 있지 않아, 내부에서 CPO 자격을 갖춘 인력을 충분히 확보하지 못하고 있으며, 이에 따라 외부 인력에 의존하는 경향이 나타나고 있다.

따라서, CPO의 경력, 교육 및 자격 요건을 종합적으로 고려한 전문성 강화 체계를 구축할 필요가 있다. 특히 개인정보보호 담당자가 실무 경험을 바탕으로 단계적으로 경력을 개발하며 CPO로 성장할 수 있도록, 교육·훈련과 경력 관리가 연계된 지원 제도의 마련이 필요하다.

4) 개인정보보호 직무에서의 AI 영향

다양한 산업에서 인공지능의 활용이 확산됨에 따라, **개인정보보호 직무에서도 AI 활용이 증가**하고 있는 추세이다. 개인정보 수집·분석, 단순 모니터링, 일부 기술 적용 등에 대해서는 AI를 활용한 자동화가 이루어지고 있으며, AI 학습 데이터에 대한 개인정보보호의 영역도 증가하고 있다.

하지만, 이와 같이 AI 기술의 확산과 함께 개인정보 처리·활용 방식이 변화하고 있음에도 불구하고, 현재 개인정보보호 직무 체계 내에서 AI 관련 업무가 어느 직무에서, 어떤 수준의 책임으로 수행되어야 하는지에 대한 체계적 정리는 아직 미흡한 상황이다.

특히, AI 학습 데이터에 포함된 개인정보의 관리, AI 기반 자동화·탐지·분석 시스템의 활용, AI 영향평가와 기존 개인정보 영향평가 간의 역할 구분, AI 기본법 시행 이후 개인정보보호 직무의 대응 범위 확대 등은 향후 개인정보보호 직무에서 핵심적으로 다루어져야 할 영역으로 판단된다. 이에 따라, **개인정보보호 직무별 AI 관련 역할과 책임 수준**을 명확히 제시하고, AI를 단순한 기술 변화가 아닌 **새로운 리스크 관리 대상으로 반영**하는 등의 직무 재정립이 필요하다.

그러나, AI 기반의 자동화가 확대된다고 해서 개인정보보호 인력의 역할이 축소된다고 보기는 어렵다. AI 활용 여부에 대한 중요 의사결정, 침해 발생 시의 판단과 책임, 조직 내부 및 외부 이해관계자와의 소통·조정 등은 자동화로 대체하기 어려운 역할이다.

따라서, 향후 개인정보보호 직무 설계 시 기존 역량과 더불어 AI 리스크를 종합적으로 해석하고 대응할 수 있는 융합 역량으로 재정립하여, 이를 뒷받침할 전문 인력 양성이 꾸준히 필요한 상황이다.

2. 제언

개인정보보호 분야는 **법·제도 변화와 기술혁신을 중심으로 빠르게 성장**하고 있다. 과거에는 개인정보보호가 법과 규제 준수 중심의 영역으로 인식되었지만, 오늘날에는 **기술적 역량을 겸비한 전문 인력**을 요구하고 있으며 보안, 데이터 거버넌스, 서비스 기획과 운영 등 **다양한 개인정보보호 역량이 요구**되고 있다.

또한, 디지털 전환이 가속화되면서 다양한 산업에서 개인정보를 활용하는 방식이 복잡해지고 있으며, 이에 따라 개인정보를 안전하게 관리하고 활용하기 위한 **기술과 가이드라인 역시 지속적으로 변화**하고 있다. 특히, 인공지능, 클라우드 등과 같은 신기술이 등장할 때마다 개인정보 처리 방식에 새로운 역량이 요구되고 있으며, 이를 규율하기 위한 각 산업에 특화된 법·제도도 신설되었다.

이렇듯 개인정보보호 분야는 **매우 빠른 주기로 변화**하고 있다. 「개인정보 보호법」 등 유관 법령의 개정 주기가 짧아지고, 기술 역시 급격히 발전하고 있다. 최근 다양한 개인정보 관련 사고 역시 개인정보보호산업 변화에 큰 영향을 미치고 있으며, 직무 종사자의 업무 범위와 요구 역량도 함께 확대되고 있는 추세이다. 이에 따라, 개인정보보호 직무 수행을 위해서는 정책 발표, 국내외 규제 논의, 기술 동향, 판례 및 감독기관의 해석 기준 등 **변화와 흐름을 지속적으로 살펴보는 것이 필수적**이다.

따라서, 개인정보보호산업을 소관하는 정보보호ISC에서는 **주기적인 직무변화 모니터링을 통해 변화를 파악**할 필요가 있다. 이러한 모니터링은 산업 종사자 및 직무 담당자들에게 변화에 선제적으로 대응할 수 있는 기반을 제공하고, 개인정보 관련 사고의 리스크를 줄이는 데에 중요한 역할을 할 것이다.

2025 개인정보보호산업 직무변화 모니터링 보고서

부 록

PART. 06

6 부 록

1. 직무변화 모니터링 설문지

직무변화 모니터링

(인사 및 현업부서 대상 CATI 조사)

안녕하십니까?
정보보호 인적자원개발위원회는 고용노동부에서 지원하는 산업 거버넌스로서 직업능력개발의 기초정보를 제공하기 위한 다양한 사업을 수행하고 있습니다.

본 위원회에서는 금년도 사업 가운데 하나로 「직무변화 모니터링」 사업을 수행하고 있으며, 이를 위해 개인정보보호산업의 기업 관계자를 대상으로 '직무변화 모니터링'을 실시하고 있습니다.

이번 모니터링을 통해 정보보호산업의 직무변화 양상을 파악하고 그에 따른 역량 변화에 대응하기 위한 시사점을 도출하고자 합니다.

귀하의 소중한 의견은 직업능력개발의 발전을 위한 자료로 활용될 예정이니 잠시 시간을 내어 끝까지 설문에 응답해 주시기를 당부드립니다.

응답을 완료한 경우 모니터링 완료 이후에 소정의 답례품을 지급해 드릴 예정입니다.

귀하께서 응답하신 내용은 통계 목적으로만 사용되며, 「통계법」 제33조와 34조에 의해 비밀이 보장되고 타 목적으로는 사용되지 않을 것임을 약속드립니다. 감사합니다.

2025년 11월

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

- 주관기관 : 정보보호 인적자원개발위원회(대표기관 : 한국정보보호산업협회(KISIA))
  이보연 팀장 Tel (02) 6748-2011 / 이은수 주임 Tel (02) 6418-5651

개인정보 수집 · 이용 동의 안내

개인정보보호법 등 관련 법규에 의거하여 정보보호 인적자원개발위원회(한국정보보호산업협회)는 응답자의 개인정보 수집 및 활용에 대해 개인정보 수집·이용 동의를 받고 있습니다.

해당 정보는 명시된 제공목적 이외에는 활용되지 않으며, 제공한 개인정보의 이용을 거부하고자 할 경우에는 열람·정정·삭제를 요청할 수 있습니다.

아래와 같이 민감정보를 처리합니다.

제공 항목	제공목적	보유기간
성명, 전화번호, E-mail	데이터 검증 및 오류 수정을 위한 추가 연락	'25.12.31(화)까지

본인은 위 사항에 따라 조사 사실을 충분히 설명 받고 숙지하였으며, 조사 참여를 거부할 권리가 있다는 사실을 인지하고 있으며, 개인정보 제공에 동의합니다.

동 의		비동의	

2025년 11월 일

성명 (서명 또는 인)

대표 응답자 정보			
성명		전화번호	
부서/직위		e-mail	
직무경력		휴대폰 번호 (답례품 수령)	
비고	* 조사 관련 요구 사항 있으면 기입		

A. 귀사의 일반현황 정보를 기재해 주십시오.

기업명			
대표자 성명			
소재지	① 서울 ② 부산 ③ 대구 ④ 인천 ⑤ 광주 ⑥ 대전 ⑦ 울산 ⑧ 경기 ⑨ 강원 ⑩ 충북 ⑪ 충남(세종) ⑫ 전북 ⑬ 전남 ⑭ 경북 ⑮ 경남 ⑯ 제주		
기업형태	① 대기업 ② 중견기업 ③ 중소기업 ④ 공공기관 ⑤ 협회 또는 단체 ⑥ 기타( )		
개인정보보호 제품/서비스 운영 여부	① 개인정보보호 제품/서비스 운영 ② 개인정보보호 제품/서비스 미운영 (운영 분야 :)		
사내 개인정보보호 담당 부서	① 개인정보보호 부서 운영 ② 정보보호 부서에서 개인정보보호 업무 수행 ③ 타 부서에서 개인정보보호 업무 수행 (수행 부서 :) ④ 별도의 전담 부서 없이 각 사업 부서별 개인정보보호 업무 수행 ⑤ 기타( )		
전체 종사자 수 (2025년 응답일 기준)	명 * 상시, 일용, 파견 종사자 모두 포함	개인정보보호 담당자수 (2025년 응답일 기준)	명 * 상시, 일용, 파견 종사자 모두 포함

B. 다음은 개인정보보호산업의 직무변화 선행요인과 관련된 질문입니다.

B-1. 최근 개인정보보호산업의 직무나 일하는 과정의 변화를 초래하는 요인이 무엇이라고 생각하십니까? (복수선택 가능)

① 기술혁신(인공지능, 자동화 등) ② 법제도변화
③ 인력변화(인구감소, 처우·급여 등 개인욕구변화 등) ④ 시장환경변화(시장수요, 경쟁 등)
⑤ 업무환경변화(재택근무, 스마트오피스 등) ⑥ 기타( )

B-2. B-1 응답과 관련하여, 해당 응답을 선택한 구체적인 이유는 무엇입니까?

구 분	의 견
이 유	*ex) 코로나 이후 비대면 근무방식 확산으로 개인정보 유출 위험이 증가함*

C. 다음은 직무변화의 직무별 세부내용 관련 질문입니다.

<개인정보보호 분야 직무 구분>

직무명	정의	키워드
개인정보 가명·익명처리	개인정보 가명·익명처리란 개인정보를 법령 등에 따라 정보주체의 동의 없이 안전하게 활용하기 위하여 적정한 수준으로 가명·익명처리를 수행하고 사후관리를 하는 일이다.	가명·익명 법제도 분석 / 가명·익명처리 기획 / 가명·익명 위험관리 / 가명·익명처리 / 가명정보 결합·반출 / 가명·익명처리 적정성 검토 / 가명·익명 사후관리
개인정보보호 관리	개인정보보호 관리는 개인정보 법령 및 정책을 기반으로 조직의 개인정보 보호계획 수립, 위험관리, 기술적/관리적 보호조치를 통해 개인정보 관리를 수행하는 일이다.	개인정보보호 법령·정책 분석 / 개인정보보호 기획 / 개인정보보호 위험관리 / 개인정보 분쟁조정 / 개인정보 생명주기 관리 / 개인정보 기술적 보호조치 / 개인정보 관리적 보호조치
개인정보보호 운영	개인정보보호 운영은 내부 개인정보보호 관리계획에 따라 처리시스템을 운영하고 침해/유출 사고에 대응하며 개인정보취급 업무를 수행하는 일이다.	개인정보보호 내부 관리 계획 / 개인정보 처리시스템 운영 / 수탁사 관리·감독 / 개인정보 암호화 / 개인정보 침해·유출 사고 대응 / 정보주체 권리보장
개인정보보호 컨설팅	개인정보보호 컨설팅은 개인정보보호 환경 분석 및 위험평가를 통해 보안모델을 설계하고 개인정보보호시스템 품질을 관리하여 개인정보 안전성 확보를 지원하는 일이다.	개인정보보호 환경 분석 / 개인정보보호 수준진단 계획 수립 / 개인정보보호 위험평가 / 개인정보보호 보안모델 설계 / 개인정보보호 이행계획 수립 / 개인정보보호시스템 품질 관리
개인정보 이동활용관리	개인정보 이동활용관리는 개인정보의 안전한 이동과 활용을 위해 서비스를 기획하여 운영하고 이용자를 교육하는 일이다.	개인정보 활용 서비스 기획 / 마이데이터 서비스 운영 / 데이터 안심구역 운영 / 개인정보 보호·활용 교육 / 개인정보 활용 서비스 품질관리
개인정보 인증·평가	개인정보 인증·평가는 개인정보처리자를 대상으로 개인정보보호 기준 준수 여부를 심사하고 평가하는 업무를 수행하는 일이다.	개인정보 인증심사 준비 / 개인정보 인증심사 착수 / 개인정보 관리체계 진단 / 개인정보 안전조치 진단 / 개인정보 처리단계별 보호조치 진단 / 개인정보 처리시스템 기술적 보호조치 점검 / 인증평가 보고서 작성·배포

C-1. 위와 같은 개인정보보호산업 직무 구분이 얼마나 적절하다고 생각하십니까?

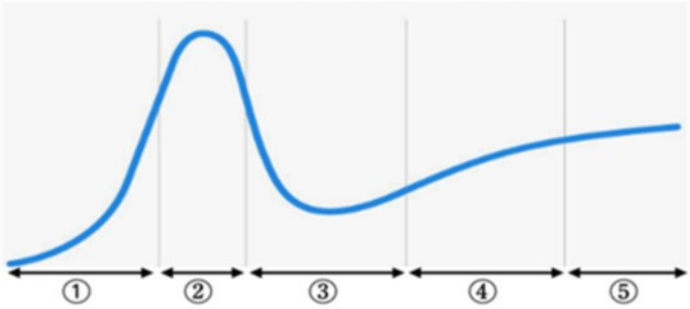
구 분	적절함	···			적절하지 않음
적절성	①	②	③	④	⑤

C-2. (C-1 ③~⑤ 응답자만) 직무가 적절하지 않다고 생각하는 이유는 무엇입니까?

① 직무내용이 현실을 잘 반영하지 못해서
② 직무 단위가 대기업 중심으로 되어 있어서
③ 과거의 직무로 현재와 달라서
④ 직무내용이 지나치게 분절되어 있어서
⑤ 직무내용이 지나치게 통합되어 있어서
⑥ 기타(　　)

C-3. 다음 직무에 대해 현재 산업 내 성숙도를 선택하여 주십시오.

[참고] 가트너의 하이프 사이클



단 계		특 징
1	촉발	· 잠재적 기술이 관심을 받기 시작하는 시기이며, 초기 단계의 개념적 모델과 미디어의 관심이 대중의 관심을 불러일으킨다. · 상용화된 제품은 없고 상업적 가치도 아직 증명되지 않은 상태이다. → 해당 업무에 대한 관심이 높아지기 시작하여, 직무의 수요가 예상되는 단계
2	기대	· 초기의 대중성이 일부의 성공적 사례와 다수의 실패 사례를 양산해 낸다. · 일부 기업이 실제 사업에 착수하지만, 대부분의 기업들은 관망한다. → 해당 업무에 대한 관심이 매우 높아져, 직무 종사자가 나타나기 시작하는 단계
3	환멸	· 실험 및 구현이 결과물을 내놓지만 실패함에 따라 관심이 시들해진다. · 제품화를 시도한 주체들은 포기하거나 실패한다. · 살아남은 사업 주체들이 소비자들을 만족시킬만한 제품의 향상에 성공한 경우에만 투자가 지속된다. → 해당 업무에 대한 관심이 시들해짐에 따라, 일부 회사에서만 직무 담당자를 지정하는 단계
4	계몽	· 기술의 수익 모델을 보여 주는 좋은 사례들이 늘어나고 더 잘 이해되기 시작한다. · 2-3세대 제품들이 출시된다. · 더 많은 기업들이 사업에 투자하기 시작한다. · 보수적인 기업들은 여전히 유보적인 입장을 취한다. → 해당 업무가 인정받기 시작하여, 다수의 회사에서 직무 담당자를 보유하기 시작하는 단계
5	안정	· 기술이 시장의 주류로 자리 잡기 시작한다. · 사업자의 생존 가능성을 평가하기 위한 기준이 명확해진다. · 시장에서 성과를 거두기 시작한다. → 해당 업무가 자리 잡기 시작함에 따라, 다수의 회사에서 직무 담당자를 안정적으로 보유하는 단계

직 무	촉발	기대	환멸	계몽	안정
개인정보 가명·익명처리	①	②	③	④	⑤
개인정보보호 관리	①	②	③	④	⑤
개인정보보호 운영	①	②	③	④	⑤
개인정보보호 컨설팅	①	②	③	④	⑤
개인정보 이동활용관리	①	②	③	④	⑤
개인정보 인증·평가	①	②	③	④	⑤

C-4. 다음 직무에 대해 전체 인력의 수준을 범위로 선택하여 주십시오.
(예시 : 개인정보 가명·익명처리 ④~⑧, 개인정보보호 관리 ⑤~⑧ 등)

직 무	1	2	3	4	5	6	7	8
개인정보 가명·익명처리	①	②	③	④	⑤	⑥	⑦	⑧
개인정보보호 관리	①	②	③	④	⑤	⑥	⑦	⑧
개인정보보호 운영	①	②	③	④	⑤	⑥	⑦	⑧
개인정보보호 컨설팅	①	②	③	④	⑤	⑥	⑦	⑧
개인정보 이동활용관리	①	②	③	④	⑤	⑥	⑦	⑧
개인정보 인증·평가	①	②	③	④	⑤	⑥	⑦	⑧

[참고] 수준별 특징

수준	특 징	수준	특 징
1	· 단순하고 반복적인 과업 수행	5	· 경력 : 약 11년~14년 (4수준 + 1~3년) · 매우 복잡하고 비일상적인 과업 수행 · 타인에게 지식 전달 가능
2	· 경력 : 약 1년 (1수준 + 6개월~12개월) · 절차화되고 일상적인 과업 수행	6	· 경력 : 약 15년~17년 (5수준 + 1~3년) · 다양한 과업 수행 · 타인에게 지식 및 노하우 전달 가능
3	· 경력 : 약 2~5년 (2수준 + 1~3년) · 다소 복잡한 과업 수행	7	· 경력 : 약 19년~21년 (6수준 + 2~4년) · 광범위한 작업 수행 · 타인의 결과에 대한 의무 및 책임
4	· 경력 : 약 6~10년 (3수준 + 1~4년) · 복잡하고 다양한 과업 수행	8	· 경력 : 약 23년~25년 (7수준 + 2~4년) · 광범위한 기술적 작업 수행 · 조직 및 업무 전반에 대한 권한 및 책임

C-5. 다음 문항에 대해 지난 5년간의 전체적인 직무 변화도를 선택하여 주십시오.

직 무	전혀 달라지지 않음	· · ·			완전히 달라짐
개인정보 가명·익명처리	①	②	③	④	⑤
개인정보보호 관리	①	②	③	④	⑤
개인정보보호 운영	①	②	③	④	⑤
개인정보보호 컨설팅	①	②	③	④	⑤
개인정보 이동활용관리	①	②	③	④	⑤
개인정보 인증·평가	①	②	③	④	⑤

C-6. (C-5 ②~⑤ 응답자 중, 해당 직무에만 응답) 각 직무별 변화 요인은 무엇이라고 생각하십니까? (복수선택 가능)

직 무	기술혁신	법·제도 변화	인력변화	시장환경 변화	업무환경 변화
개인정보 가명·익명처리	①	②	③	④	⑤
개인정보보호 관리	①	②	③	④	⑤
개인정보보호 운영	①	②	③	④	⑤
개인정보보호 컨설팅	①	②	③	④	⑤
개인정보 이동활용관리	①	②	③	④	⑤
개인정보 인증·평가	①	②	③	④	⑤

C-7. C-6 응답 이외의 각 직무별 기타 변화 요인이 있다면 무엇입니까? (해당 직무에만 응답)

직 무	기타 요인

C-8. 다음 문항에 대해 향후 5년 이내 인력수요 전망을 선택하여 주십시오.

직 무	매우 높음	높음	보통	낮음	매우 낮음
개인정보 가명·익명처리	①	②	③	④	⑤
개인정보보호 관리	①	②	③	④	⑤
개인정보보호 운영	①	②	③	④	⑤
개인정보보호 컨설팅	①	②	③	④	⑤
개인정보 이동활용관리	①	②	③	④	⑤
개인정보 인증·평가	①	②	③	④	⑤

C-9. 현재 구분된 직무 외에 새롭게 생겨난 직무(신생직무)나 사라진 직무(소멸직무), 통합.분할 등 대체되고 있는 직무(대체직무)가 있다면 관련하여 자유롭게 작성하여 주시기 바랍니다.

구 분	직 무
신생직무	
소멸직무	
대체직무	

D. 개인정보보호 분야의 직무구분 및 정의, 직무변화 요인, 직무변화 양상 등 직무 및 직무변화와 관련하여 기타의견이 있으면 자유롭게 작성하여 주시기 바랍니다.

구 분	의 견
기타의견	

☺ 설문에 응답해 주셔서 감사합니다 ☺

2025 개인정보보호산업 직무변화 모니터링 보고서

발 행 일 2025년 12월

발 행 처 정보보호 인적자원개발위원회
(대표기관: 한국정보보호산업협회)

주 소 서울시 송파구 중대로 135, IT벤처타워 서관 14층
정보보호 인적자원개발위원회 사무국

전 화 (02) 6748-2011

〈비매품〉

2025

개인정보보호산업 직무변화 모니터링 보고서