



PIA 개인정보 영향평가

작성자 : *Eric Yoon*

목 차

- 1. 개인정보 영향도 등급
- 2. PDCA 사이클
- 3. 거버넌스
- 4. 컴플라이언스
- 5. 관리적, 물리적, 기술적 보호조치 보충설명
- 6. PIA 개인정보 영향평가
- 7. 흐름도 작성 예시 및 실습.
- 8. 주요 용어 정리

개인정보 등급 분류시 고려할 요소

1. 개인정보 영향도 등급

자산가치	5점	1등급	비밀	주민번호, 신용카드정보, 금융정보, I D, 비밀번호, 지문, 홍채정보, 등등
자산가치	3점	2등급	대외비(조합정보)	성명+전화번호+주소+e-mail, 성명+생년월일+e-mail,.
자산가치	1점	3등급	대외비(식별어려운정보)	몸무게+키 , 주소, 학력

- 2. 법적통제 요구사항
- 3. 유출시 위험성 및 파급 영향
- 4. 정보 민감도
- 5. 정보의 고유성 및 식별성

PDCA 사이클기반

- PDCA 가 무엇인지 짚고 넘어 가보자.
- Plan,Do,Check,Act 의 반복 사이클 로써,
지속적이고 반복적인 개선 활동을 요구한다.
- 개인정보 보호 관리과정 이다
- 조직구성,위험관리,모니터링감사,정책
- 1.계획plan (①.정책수립,관리범위정함 ②.관리범위내의개인정보자산식별 ③.개인정보흐름파악및 흐름도 작성 ④.개인정보처리상에 문제점 파악.)
- 2.실행do (①.식별된 정보자산을 바탕으로 위험평가 실시 ②.정보보호대책의 수립과 이행)
- 3.검증check (①.정보보호대책의 효과성확인 ②.모니터링 정기적인점검,감사실시등으로 체크)
- 4. 개선 act (잔여 위험에 대한 추가적인 조치사항 반영)**반영=순환 PDCA**

거버넌스 와 컴플라이언스 를 이해하고 나가자

○ 거버넌스 (governance) 란 무엇일까 ?

정부 와 비슷하지않은가 ???

○ 국가의 여러업무를 관리하기위해 정치,경제및 행정적권환을 행사하는방식으로써,

일종의 국정관리 체계라고 의미를 생각하자.

현재,우리는 정보보안을 말하고 있으므로 IT, Security 법,명령등을 준수 한다라고 해석 하면될것같다.

IT 거버넌스 와 컴플라이언스 ,

Security 거버넌스 와 컴플라이언스 에 대해 알아보도록 하자.

거버넌스

거버넌스(Governance)

IT Governance

정보기술(IT) 자원과 정보, 조직을 기업의 경영 전략 및 목표와 연계

경쟁 우위를 확보

의사결정 및 책임에 관한 프레임워크

이사회와 경영진의 책임 아래 수행되는 기업 지배 구조의 일부로 존재

리더십, 조직 구조, 프로세스 통제, 관리 체제로 구성

Security
Governance

IT Governance

거버넌스(Governance)

Security
Governance

최고 경영층의 정보보호에 대한 전략과 통제체계를 규정하는 보안정책 체계

정보보호는 기술적인 이슈가 아닌 전략적 이슈

법적인 문제임을 인식하는 것

정보보호에 대한 지시와 통제 수행

컴플라이언스 ?

컴플라이언스(Compliance)

IT Compliance

Security
Compliance

각종 법, 제도적 규제 및 권고의 철저한 대응

각 나라별, 글로벌 감독당국이 제시한 각종 요건 만족

기업의 정보시스템과 업무프로세스 재정비

컴플라이언스(Compliance)

IT Compliance

Security
Compliance

각종 법, 제도적 규제 및 권고의 철저한 대응

해당되는 법, 규제 요건 만족

기업의 정보보호 관리 프레임워크 구축, 운영

Governance 강화 측면

개인정보 법규제의
강화에 맞춘
보안관리 노력 필요

Compliance 강화 측면

ISMS 인증 의무화
대상자에 대한
강화된 정보보호 노력 요구

정보보호의 노력

법적으로 인정

정보보호 관리증적
(Evidence)

정보보호 관리
업무프로세스 정립

- 정보보호를 위해서는 거버넌스와 컴플라이언스의 강화가 필요하다.

인증의 필요성

법률 등 컴플라이언스 측면

1

거버넌스(Governance) 강화 측면

- 영업비밀보호법으로부터 보호받기 위한 **회사의 보안관리 노력 강구**
- 법인 또는 개인이 위반 행위를 방지하기 위해 해당 업무에 관해 주의와 감독을 게을리하지 않은 경우 **양벌 규정에 대한 예외 적용**

2

개인정보 포함 인터넷 침해사고에 관련된 컴플라이언스(Compliance) 측면

- 정보통신서비스제공자는 **정보통신망법의 의무를 충실히 이행**
- 교육, 의료, 공공 부문 등 개인정보를 취급하는 모든 경우에는 **개인정보보호법을 지켜야 함**

인증의 필요성

법률 등 컴플라이언스 측면

3 2013년부터 정보통신망법 시행에 따른 정보보호 관리체계(ISMS) 인증제도 의무화

➤ 기존 안전진단 대상 사업자들은 강화된 정보보호 관리체계 인증을 의무적으로 받아야 함

4 개인정보보호법 및 정보통신망법 등 정보보호 관련 법률 강화

5 사회적으로 정보보호체계 수립 및 이행에 대한 요구 강화

구성요소 다시 확인 ! 관리적, 물리적, 기술적 보호대책 !!! 필수 !! 학습 하자 !!!

PIMS 구성요소

관리과정 요구사항

관리체계 수립 (정책, 범위, 조직 등)
실행 및 운영 (개인정보 식별, 위험관리, 구현 등)
검토 및 모니터링 (사후관리)
교정 및 개선 (개선활동, 교육)

생명주기 및 권리보장 요구사항

생명주기 관리 (수집, 이용 및 제공, 보유, 파기)
정보주체 권리보장

보호대책 요구사항

관리적 (인적, 침해사고)
기술적 (접근권한, 접근통제, 운영보안, 암호화, 개발보안)
물리적 (영상정보처리기기, 물리적 보안, 매체)

- 알고보면 보이고 모르고 보면 안보이기때문에 다시 보고 또 보도록 하자
- 보안인이라면 꼭 알아야될 보호대책 다시 짚어보자.

관리적 보호조치 는 무엇인가 ?

1. 교육 및 훈련 - 최소 연 1회 이상 !
2. 개인정보 취급자 관리-취급자 감독, 보안서약서, 퇴직자 등 직무변경관리
3. 위탁업무관리 및 침해사고관리- 외부위탁계약, 정부주체고지. 위탁자관리감독
(위탁계약서에 반드시 포함할 사항이 아닌것은 ?
수탁자가 접근가능한 개인정보의 범위 및 유형은 반드시 계약서에 포함하지 않아도 된다.)-시험문제 자주출제됨.
4. 침해사고관리- 침해사고 대응절차 및 체계구축, 침해사고 훈련개선, 대응

물리적 보호조치 는 무엇인가 ?

- 1. 물리적 보안 – 보호구역지정 및 관리, 보호설비 설치, 출입 통제 등...
- 2. 영상 정보 처리기기 관리
- 3. 매체 관리- 저장매체파기, 재사용시....-데이터 복구 안되도록...

기술적 보호조치 는 무엇인가 ?

♡ 개인정보 처리시스템과 관련 시스템의 계정과 권한은 필요한 사람에게 최소한으로 부여 되어야하며, 권한부여 이력은 일정 기간 보관 - 개보3년, 망5년

♡ 개인정보 처리시스템 접속기록은 법령에 따라 일정기간 이상 보관하여야 하며 , 권한 없는자의 접근시도, 권한의 오남용, 시스템 오류등을 적발하기 위하여 주기적으로 접속 기록을 검토 하여야함.

♡ 계정의 비밀번호를 안전하게 관리 하기 위한 기준을 마련하여 이행하여야 하며 , 필요한경우 개인정보 취급자의 단말을 망분리 해야함.

기술적 보호조치 는 무엇인가 ?

♥망법에서 망분리대상자는

- 개인정보 처리시스템으로 부터 다운로드할수 있는 권한을 보유한자
- 개인정보처리시스템을 이용하는 개인정보 취급자의 권한을부여,변경할수 있는자
- 개인정보 처리시스템에 저장된 개인정보를 삭제할수 있는자

♥개인정보 처리업무에 사용하는 단말과 시스템은 악성코드감염에 수행해야하며,시스템과 단말기 보호를 위해 필요한 보안 시스템을 구축하여 운영해야함.

♥개인정보 처리시스템과 관련 시스템을 개발하는 경우 개발 보안 요구사항정의,개발과,운영환경의분리,실데이터의 테스트 환경사용금지,외주개발시 용역업체관리등의 사항을 준수하여야함.

기술적 보호조치 는 무엇인가 ?

○ 1. 접근통제

- 문서로 공식화 , - 인사이동에 따른 권한변경보관-개보법3년,망법 5년 - 비밀번호관리 , -접속기록,-전자적기록, 수기문서 X
- 철저한 네트워크 관리 - 물리적,논리적 분리

○ ①. 분리운영

- 외부접근가능한서버 =DMZ망
- DB서버들은 내부망
- 내부망도 DB서는 가급적 별도의 네트워크로구분
- 개발,테스트 서버등 별도 분리
- 내부망은 가급적 사설 ip 사용

○ ②. 원격접속관리 -VPN

- 개인정보처리시스템을 외부에서 접속하여 사용하는 경우 전용선,vpn 등 사용하여 통제
- Vpn 사용시 추가 인증수단, 단말기 보안등을 고려
- ♥-개보법vpn = 안전한접속수단=암호화통신방법
- 망법vpn=안전한 인증수단=otp,ip주소인증등

○ ③.무선 네트워크 사용

- 내부용,외부용(guest용) 구분
- 비밀번호 설정 ssid 숨김 등으로 내부 메의 외부노출 최소화
- 응용 프로그램 (- 계정관리처럼 권한제한및 관리 , 멀티 로그인금지 , 세션종료시간 설정등의 보안 대책 마련)
- 데이터 베이스 관리
- 개인정보 망분리

기술적 보호조치 는 무엇인가 ?

○ 2. 운영보안

- 악성코드통제
- 취약점 점검
- 표시제한,마스킹, -비식별
- 보안시스템운영
- 노트북,모바일기기 접근관리
- 기타 운영보안-백업,복구

기술적 보호조치 는 무엇인가 ?

3. 암호화 및 개발보안등

- 암호정책 수립및 이행.
- 알고리즘 - ① 일방향암호화 -sha256 이상의 안전성 가진 방법 추천
(비밀번호 !! 무조건 일방향 !!!) sha 중에서도 80 비트 는 전혀 권장사항 아님!!! 유효기간도 만료됨 !! 128 비트 이상 사용 할것 !!
 - ② 양방향암호화-aes128 알고리즘 등 권고
- 암호키 = 안전한곳 보관
- 개인정보 개발,유지보수



○ 본격적으로 PIA 공부 합시다 !

○ PIA 개인정보 영향평가 에 대해 깊이 알아보도록 하자.

PIA 개인정보 영향평가 무엇인가요 ?

개념

개인정보를 활용하는 새로운 정보시스템의 도입 및 기존 정보시스템의 중요한 변경 시, 시스템의 구축·운영이 기업의 고객은 물론 국민의 프라이버시에 미칠 영향에 대하여 미리 조사·분석·평가하는 체계적인 절차

영향평가 목적 및 필요성

개인정보 처리자가 수반되는 사업을 추진시 해당 사업이 개인정보에 미치는 영향을 사전에 분석하고 이에대한 개선방안을 수립하여 본사업 수행시 개인정보침해사고를 사전에 예방하기 위함이다.

PIA 개인정보 영향평가 무엇인가요 ?

○ 평가대상

- 개인정보를 취급하는 시스템의 신규 구축사업
- 개인정보를 취급하는 기존 시스템을 변경하는 사업
- 개인정보보호법 제2조제6호에 따른 공공기관에서 운영하는 개인정보파일과 해당 처리시스템으로서, 개인정보파일이 개인정보보호법 시행령 제35조에 해당하는 경우 개인정보 영향평가를 의무적으로 수행하여야 합니다.

수행주체

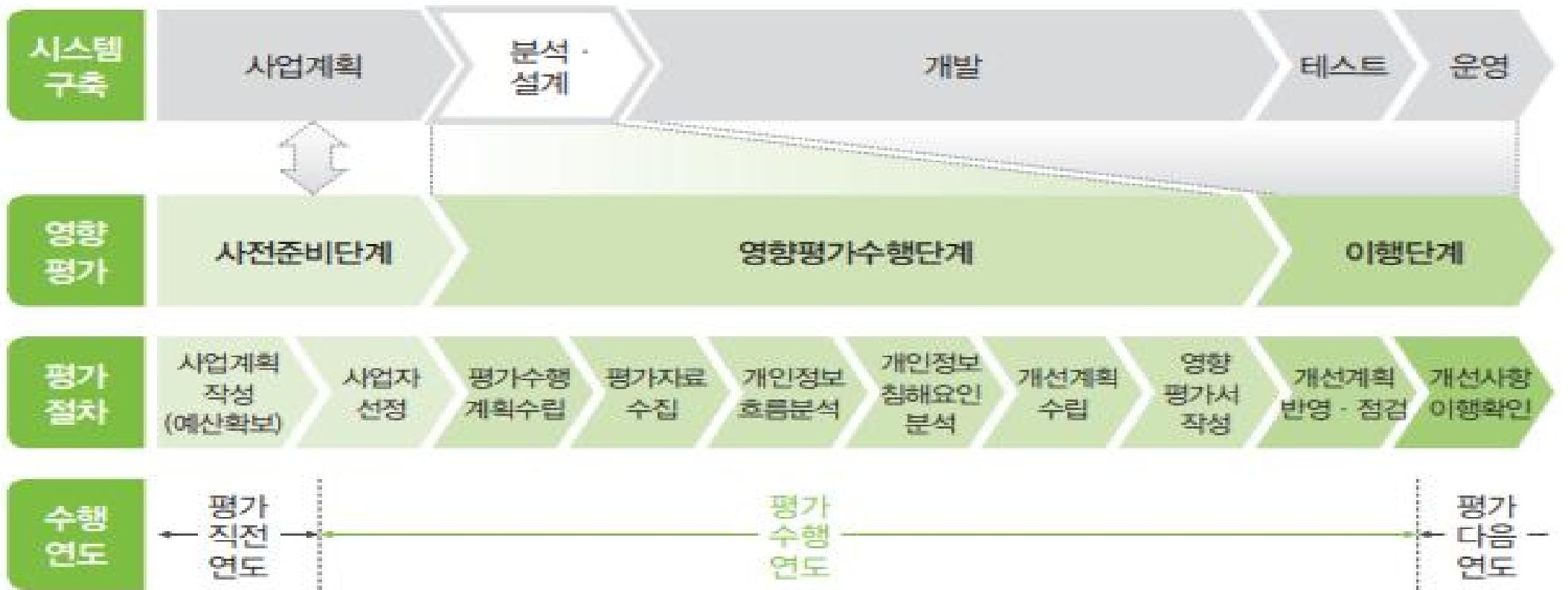
- 영향평가 주관부서 담당자, 개인정보보호 책임자, 개인정보보호 담당자 등으로 영향평가팀을 구성하여 영향평가를 수행합니다.
- ※ 공공기관은 행정안전부 장관이 지정한 평가기관에 영향평가를 의뢰하여야 합니다.

≡ 일정규모 이상의 개인정보를 전자적으로 처리하는 개인정보파일을 구축·운영 또는 변경하려는 공공기관은 「개인정보 보호법」 (이하 “법”이라 한다) 제33조 및 「개인정보 보호법 시행령」 (이하 “령”이라 한다) 제35조에 근거하여 영향평가를 수행

- (5만명 조건) 5만명 이상의 정보주체의 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
- (50만명 조건) 해당 공공기관의 내부 또는 외부의 다른 개인정보파일과 연계하려는 경우로서, 연계 결과 정보주체의 수가 50만 명 이상인 개인정보파일
- (100만명 조건) 100만 명 이상의 정보주체 수를 포함하고 있는 개인정보파일
 - ※ 현시점 기준으로 영향평가 대상은 아니나 가까운 시점(1년 이내)에 정보주체의 수가 기준을 초과할 것이 확실한 경우, 영향평가를 수행할 것을 권고
- (변경 시) 영제35조에 근거하여 영향평가를 실시한 기관이 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우, 변경된 부분에 대해서는 영향평가를 실시
 - ※ 법령상 규정된 대상시스템이 아니더라도 대량의 개인정보나 민감한 개인정보를 수집·이용하는 기관은 개인정보 유출 및 오·남용으로 인한 사회적 피해를 막기 위해 영향평가 수행 가능

영향 평가 시기

영향평가 시기



영향 평가 시기

1. 시스템을 **신규구축** 또는 기존시스템을 **변경** 하는 경우

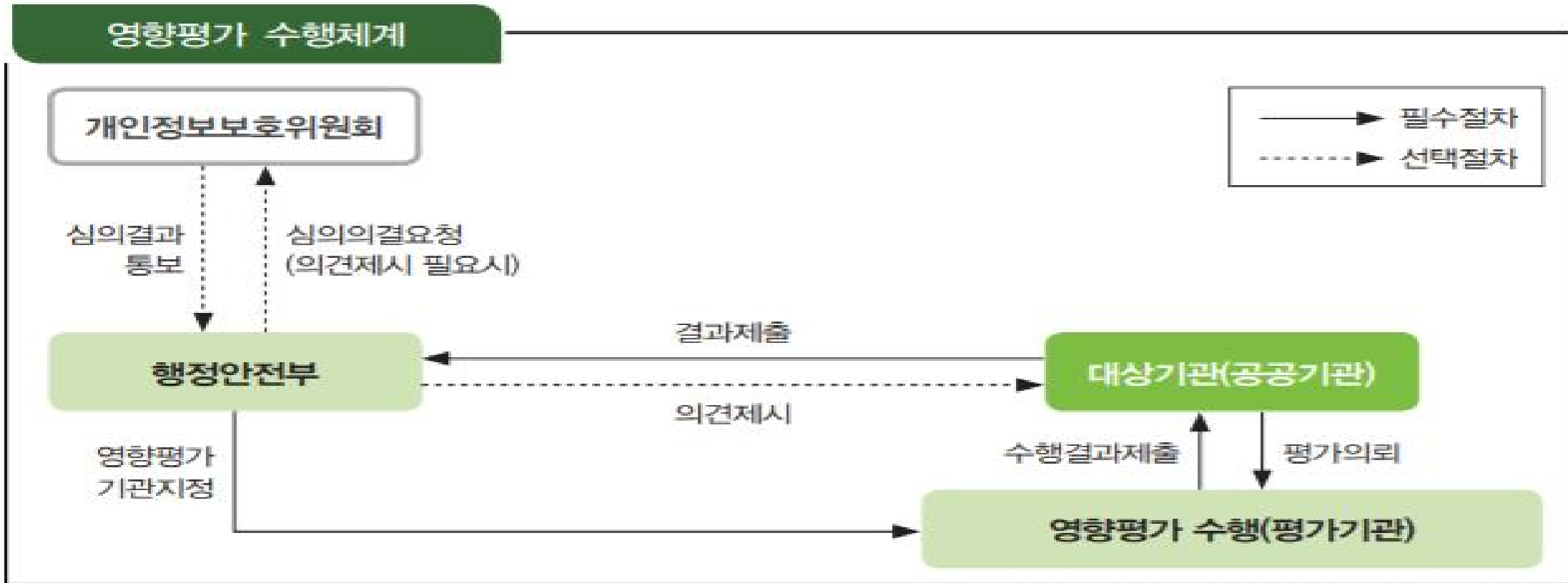
개인정보처리시스템을 신규로 구축 하거나 기존 시스템을 변경하려는 기관은 사업계획 단계에서 영향평가 의무대상 여부를 파악하여 예산을 확보한 후 대상 시스템의 설계 완료 전에 영향평가를 수행해야, 함 또한 영향평가 결과는 시스템 설계개발 시 반영해야 함 (개인정보 영향평가에 관한 고시)

2. 기 구축되어 운영 중인 시스템의 경우

개인정보처리시스템을 기 구축 운영 중 아래의 경우 추가적으로 영향평가 수행 가능

- 수집 이용 및 관리상에 **중대한 침해위험의 발생이 우려되는 경우** .
- 전반적인 개인정보 보호체계를 **점검하여 개선하기 위한 경우**

개인정보 영향평가 수행체계

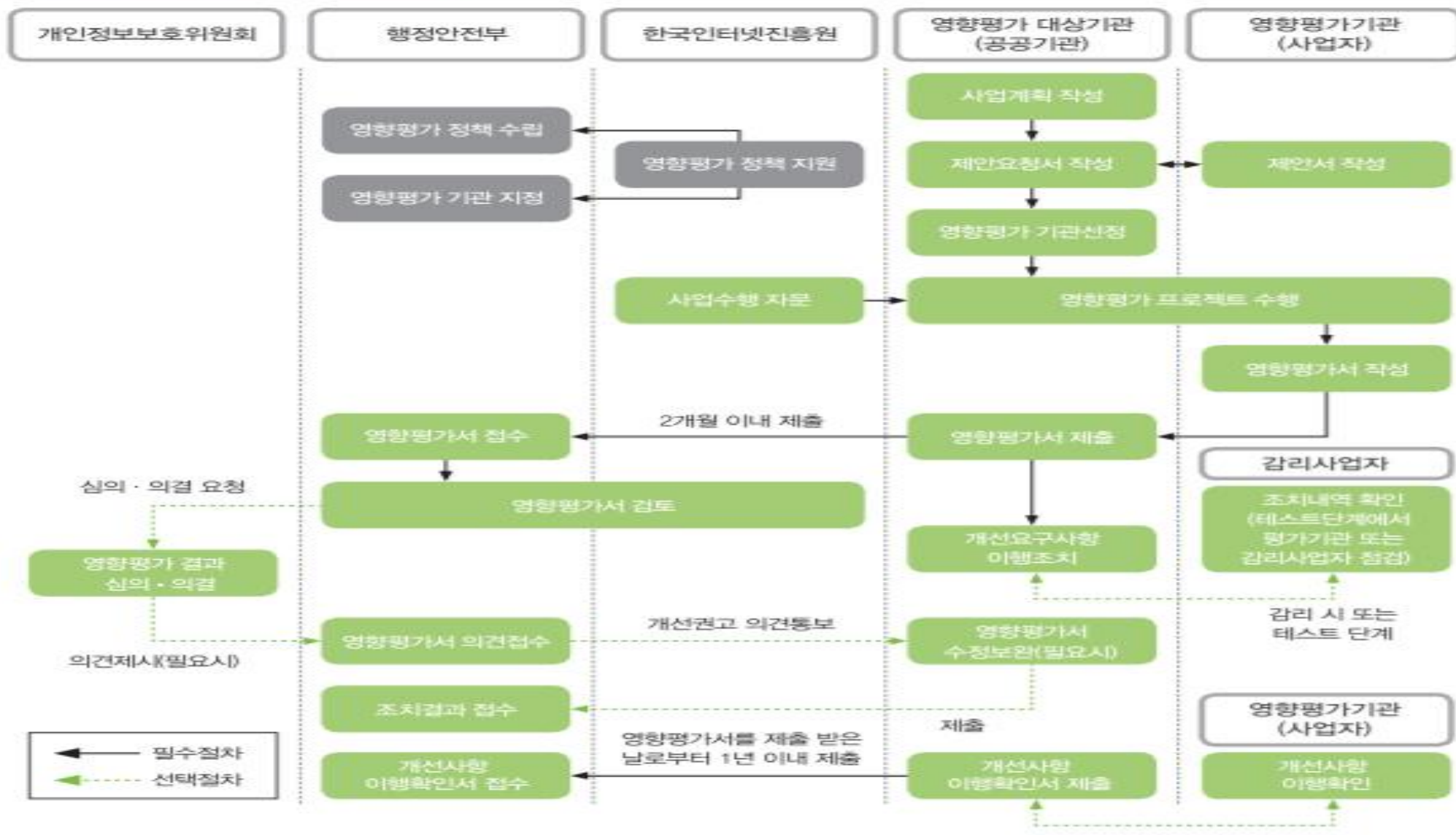


- 영향평가는 행정안전부장관이 지정한 영향평가기관에 의뢰하여 영향평가를 수행하고 그 **결과를 사업 완료 후 2개월 이내에** 행정안전부장관에게 제출
- 행정안전부장관은 개인정보보호위원회의 심의 의결을 거쳐 해당 사업에 대한 의견 제시 가능

PIA 개인정보 영향평가 수행절차 요약

- 영향평가 사업은 직전연도에 예산을 확보하고 당해연도에 평가기관을 선정하여 대상기관과, 평가기관이 협업을 통해 영향평가서를 완성
 - 영향평가서는 최종 제출받은 날로부터 2개월 이내에 행정안전부장관에게 제출
 - 영향평가서를 제출한 날로부터 1년 이내에 개선사항 이행확인서를 행정안전부장관에게 제출

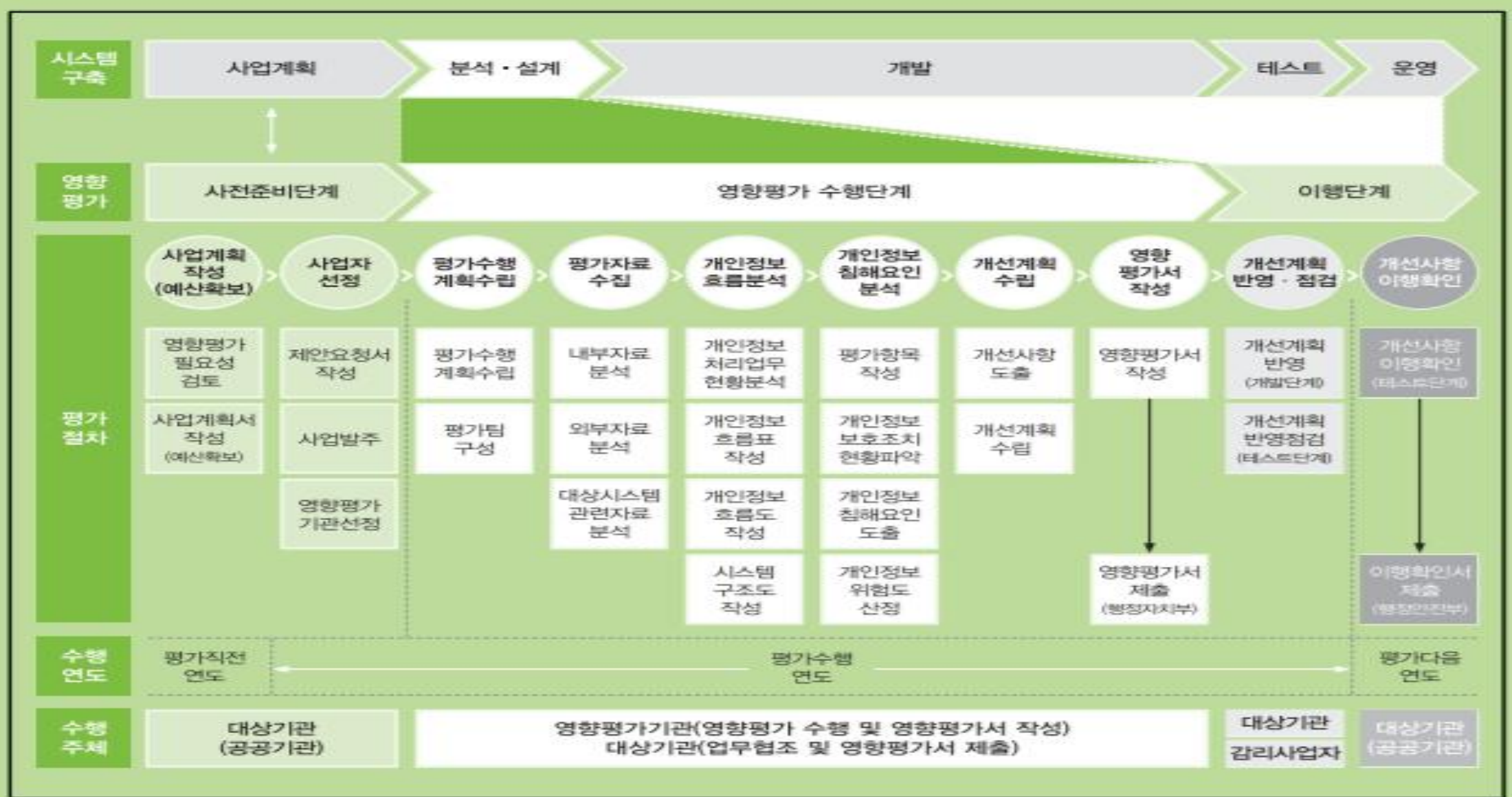
영향평가 수행 절차도



PIA 영향평가 수행절차

- 영향평가 사업은 사전준비 단계, 수행단계, 이행단계 등 3 단계로 구성
 - 영향평가 사전준비 단계 : 영향평가 사업계획을 수립하여 예산을 확보하고 평가기관을 선정
 - 영향평가 수행단계 : 선정된 평가기관이 개인정보 침해요인을 분석하고 개선계획을 수립하여 영향평가서를 작성
 - 이행 단계 : 영향평가서의 침해요인에 대한 개선계획을 반영하고 이를 점검

[영향평가 절차]



개인정보 흐름 분석

개인정보 흐름분석은 4 단계로 진행

1.개인정보 처리업무 분석

- 영향평가 대상 업무중에서 개인정보 처리업무를 도출하여 평가범위를 산정
- 개인정보를처리(수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등)하는 모든 업무를 파악한다.

2.개인정보 흐름표 작성

- 개인정보의 수집, 보유, 이용, 제공 파기에 이르는life-cycle별 현황을 식별하여 개인정보처리현황을 명확히 알수있도록 흐름표를 작성한다.

3.개인정보 흐름도 작성

- 개인정보 흐름표를 바탕으로 개인정보의 수집, 보유, 이용, 제공, 파기에 이르는 life-cycle 별 현황을 식별하여 개인정보 처리현황을 명확히 알수있도록 흐름도를 작성.

4.정보시스템 구조도 작성

- 개인정보 처리시스템,개인정보내.외부 연계시스템 및 관련 이프라의 구성을 파악.
- 다른 단계와 병렬 진행 가능하며 분석 초기에 작성하여 타 단계 진행 시 참고 가능

※ 흐름분석 및 개선계획 수립 단계와 관련하여 본 수행안내서에서 제시된 양식(표,그림 등)은 예시로서, 영향평가 기관의 자체 방법론에 따라 대상 사업의 특성 등을 고려하여 양식을 추가 또는 일부 변형하여 사용할 수 있음

(단 각 단계별 기본 절차는 준수하여야 하며 영향평가 품질 측면에서 각 절차의 취지 및 목적을 달성할 수 있도록 하여야 함)

개인정보 흐름 분석 단계 별 세부 절차

단계

개인정보 처리업무
현황 분석

개인정보
흐름표 작성

개인정보
흐름도 작성

정보시스템
구조도 작성

절차

산출물 분석
(요건정의, 설계서 등)

담당자 인터뷰
(가능한 경우, 실사)

개인정보 처리
업무 식별

개인정보 영향도
등급표 작성

개인정보 처리
업무표 작성

업무 흐름도 작성

개인정보 취급업무표
및 업무 흐름도 분석

처리단계별
업무 흐름 분류

개인정보
흐름표 작성

개인정보
흐름표 분석

개인정보
흐름도 작성
(총괄 및 취급업무별)

네트워크 및 시스템
구성 파악

보안시스템
현황 분석

정보시스템
구조도 및
정보보호 현황표 작성

영향평가서에 산출물로 기록 필요

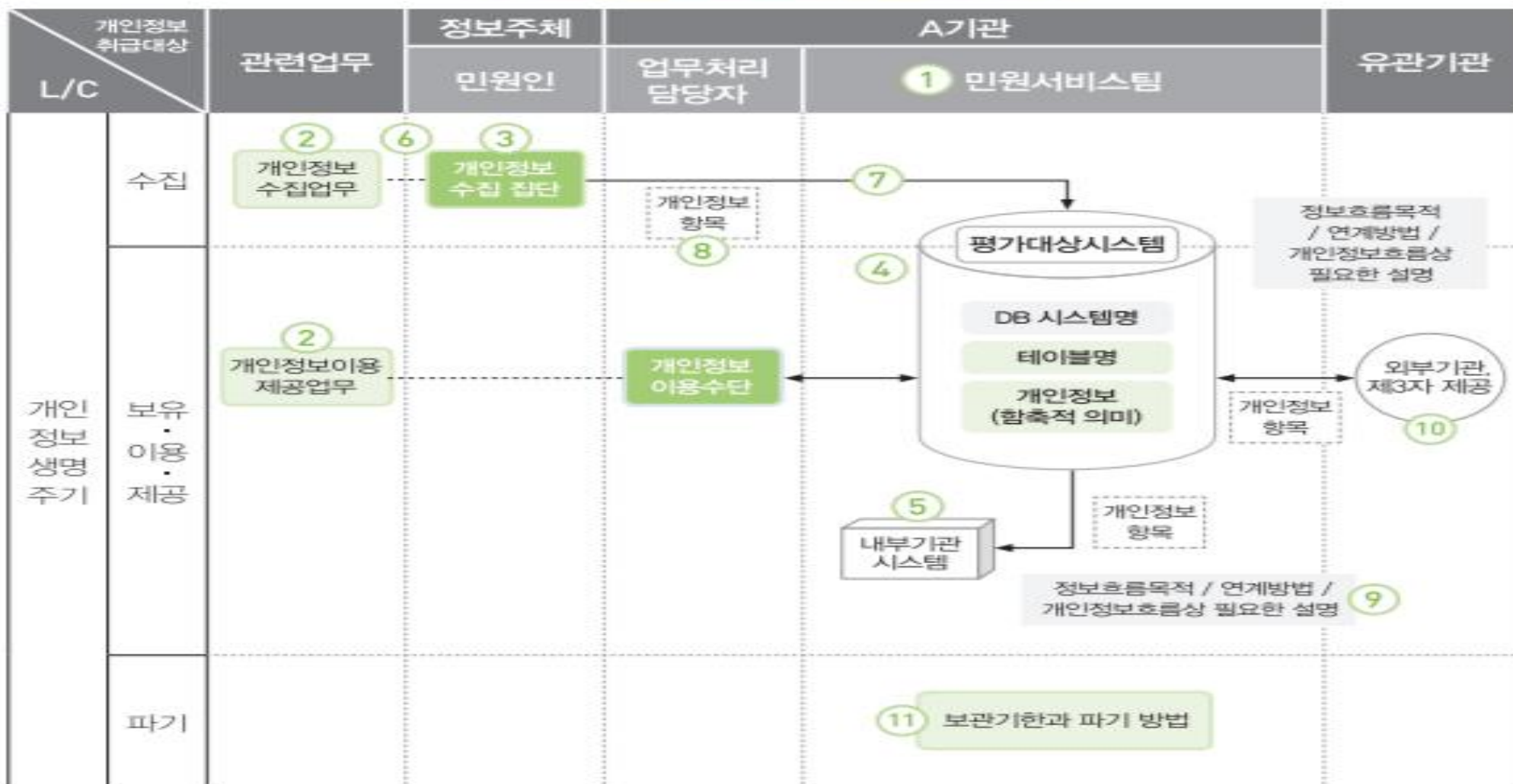
흐름도 작성 연습 해보기

다음장에는 흐름도의 예시가 있습니다.

부담없이 흐름도 작성을 해보기 바랍니다.

총괄 개인정보 흐름도 범례

평가대상 시스템 또는 평가대상 사업



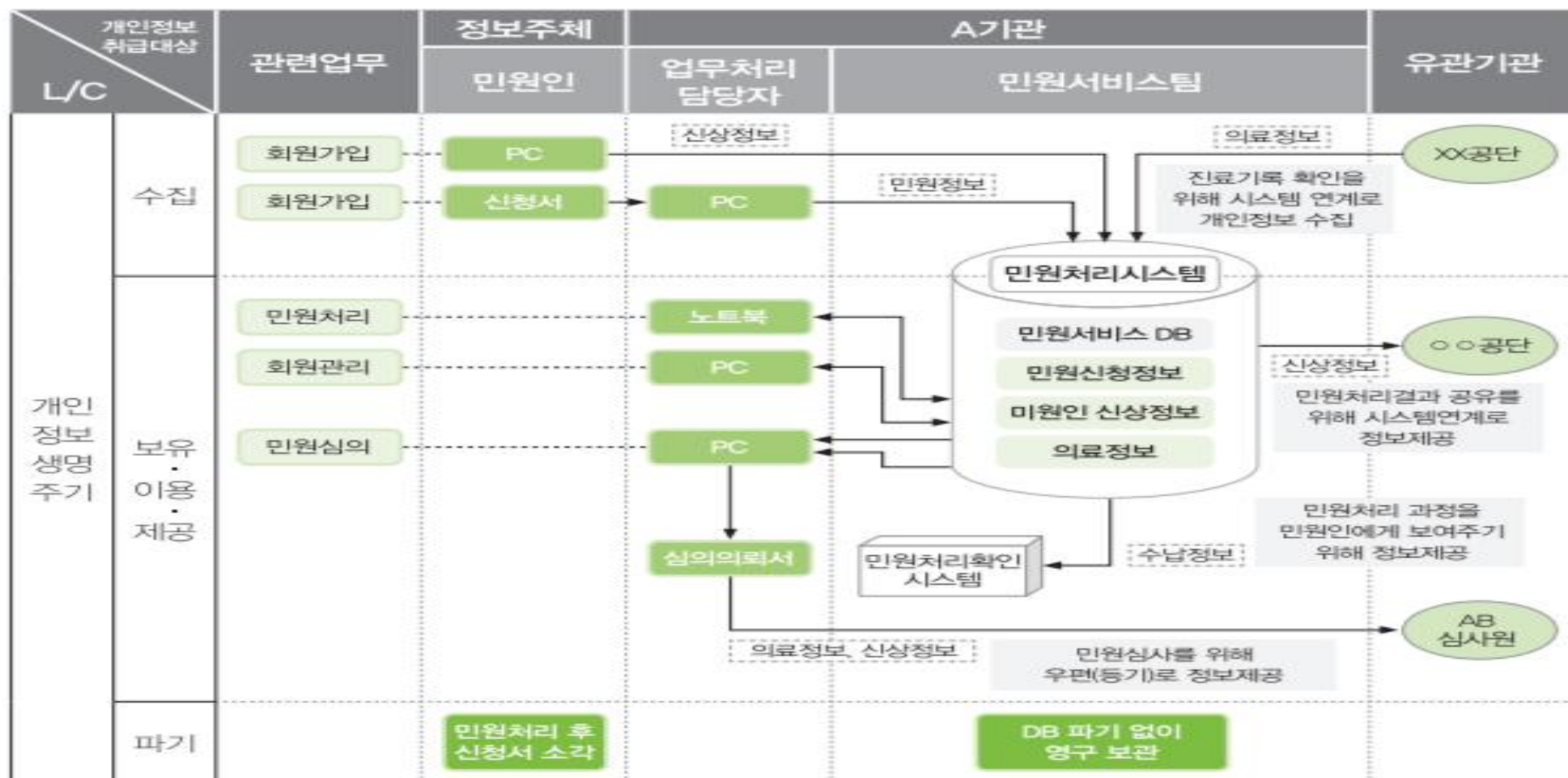
Ⅲ. 총괄 개인정보 흐름도 작성도법에 걸림

• 총괄 개인정보 흐름도 작성 방법

- ① 개인정보취급자(부서)를 정리하여 흐름도 상단에 기술
※ 취급부서 및 취급자는 필요에 따라 확장
- ② 개인정보 처리(수집, 보유, 이용·제공 파기)업무 기술
※ 업무에 따라 흐름도를 분리해야 할 경우, 각각 나누어 작성 가능
- ③ 각 업무에서 개인정보를 처리하는 수단 기술
※ 예 : PC, 신청서, 노트북, 전화, 대면, 의료기구 등
- ④ 개인정보를 보유하는 DB시스템을 표현하며 평가대상 시스템, DB명, 테이블명 또는 처리하는 개인정보의 함축적 의미를 가진 정보항목 기술
※ 예 : 신상정보(이름, 주민등록번호, 주소, 전화번호 등), 의료정보(혈압, 진단내용 등)
- ⑤ 평가대상기관 내부시스템과 연계하여 이용할 경우, 시스템명 기재
- ⑥ 개인정보 수집 시 수집하는 방법을 점선과 실선으로 표시
※ 온라인은 실선으로 하며, 오프라인으로 개인정보 흐름이 발생할 경우, 점선으로 구분
- ⑦ 개인정보 처리과정에서 정보의 흐름방향을 화살표로 연결
- ⑧ 개인정보 흐름을 표시한 화살표 상에 개인정보 항목 기술
- ⑨ 개인정보 흐름 목적/연계방식 등 개인정보 흐름파악에 필요한 설명을 간략히 기술
- ⑩ 개인정보 외부제공의 경우는 외부기관명 또는 외부업체명을 기재하고 제공방식, 제공하는 개인정보 항목 기술
※ 제공방식 : 시스템 연계(VPN, EAI 등), 우편(등기), 인편, Fax, 이메일 등
- ⑪ 개인정보의 보관기한과 파기 방법 기술

민원처리시스템 총괄 개인정보 흐름도 예시

민원처리 시스템



업무별 개인정보 흐름도 범례

① 업무명 : 평가 대상 업무명

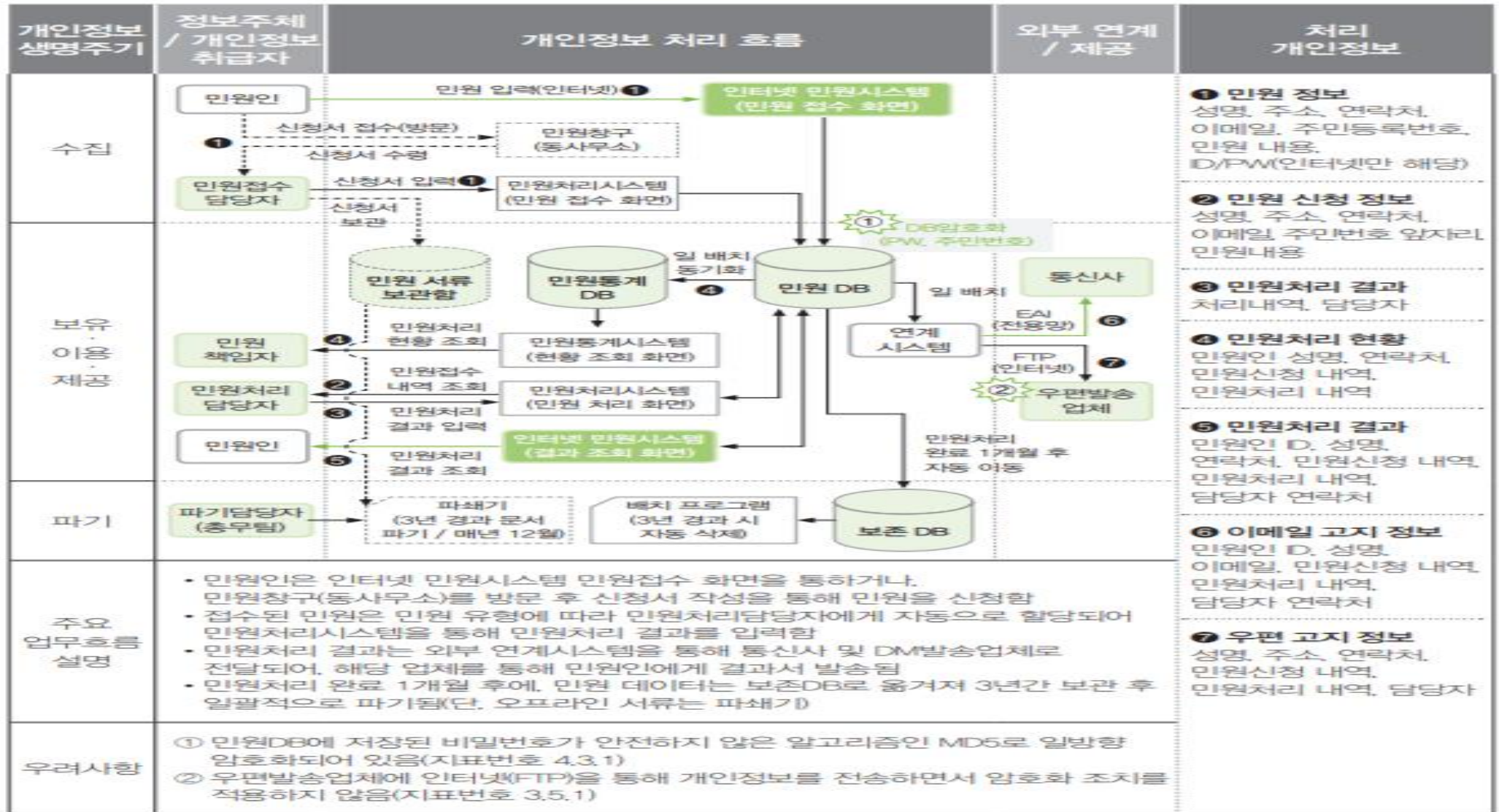
개인정보 생명주기	정보주체 / 개인정보 취급자	개인정보 처리 흐름	외부 연계 / 제공	처리 개인정보
수집	정보주체			<p>① 처리 개인정보 명칭 성명, 주소, 연락처, 주민등록번호, 이메일 등 처리되는 개인정보 항목</p>
보유· 이용· 제공	취급자		제3자/ 외부기관	<p>② 처리 개인정보 명칭 성명, 주소, 연락처, 이메일 등 처리 개인정보 항목</p> <p>③ 처리 개인정보 명칭</p>
파기				
주요 업무흐름 설명		<p>⑧</p> <ul style="list-style-type: none"> 정보주체로부터 온라인 및 오프라인을 통해 개인정보를 수집하여 각각 DB시스템 및 서류보관함에 보관함 DB시스템에 보관된 개인정보는 외부 기관으로 연계를 통해 제공됨 		
우려사항		<p>⑩</p> <p>a 외부기관과 인터넷을 통한 개인정보 제공 시, 안전 조치(암호화 전송)가 이루어지지 않음(지표번호 3.3.7)</p>		

• 업무별 개인정보 흐름도 작성 방법

- ① 평가 대상 업무명을 알기 쉽게 정의하여 흐름도 상단에 기술
- ② 정보주체 및 취급자를 식별하여 구분하여 표시
 - ※ 예 : 정보주체는 흰색 바탕, 취급자는 회색 바탕 도형 사용
- ③ 개인정보의 흐름을 간략한 세부업무 설명과 함께 점선과 실선으로 표시하고 암호화 여부를 표시
 - ※ 온라인 흐름은 실선으로 하며, 오프라인으로 개인정보 흐름이 발생할 경우, 점선으로 구분
 - ※ 암호화 된 수단을 사용하는 경우, 선을 붉은 색으로 굵게 표시
- ④ 개인정보를 처리하는 수단을 온라인 및 오프라인으로 구분하여 표시
 - ※ 온라인은 실선으로 하며, 오프라인으로 개인정보 흐름이 발생할 경우 점선으로 구분
 - ※ 외부 인터넷에서 접속 가능한 시스템의 경우, 내부 시스템과 다른 색으로 구분
- ⑤ 개인정보를 저장하는 보관소를 대표하는 명칭으로 표기하되 DB명, 파일명 또는 서류함 등과 같이 보관 방식에 따라 적절하게 용어를 선택하여 표시
 - ※ 캐비닛 등 오프라인 저장소의 경우 점선으로 구분
 - ※ 암호화 보관되는 정보의 경우 암호화 항목을 박스로 별도 표시
- ⑥ 파기방식을 파기수행 주기와 함께 온라인 및 오프라인으로 구분하여 표시
- ⑦ 개인정보 외부제공의 경우는 외부기관명(또는 외부시스템) 또는 외부 업체명을 기재하고 제공방식 및 제공하는 개인정보 항목을 기술
 - ※ 제공방식: 시스템연계(VPN, EAI 등), 우편(등기), 인편, Fax, 이메일 등
- ⑧ 평가대상 업무에 대한 흐름을 간략하게 설명하여 서술
- ⑨ 개인정보 흐름 상 전달되는 개인정보 항목을 숫자로 구분하여 도표에 표시하고 흐름도 우측에 전달되는 세부 개인정보 항목을 표시
- ⑩ 개인정보 흐름을 통해 나타난 주요 문제점 및 관련 지표번호를 요약하여 기술

민원처리 업무 개인정보 흐름도 예시

업무명 : 민원 처리



※ 각각의 평가대상 업무별로 별도의 상세 개인정보 흐름도가 작성되어야 함



다음장 부터는 위 영향평가 절차의 세부내용중 꼭

알아야될 내용들로 정리해보았다.

부담 없이 가볍게 읽어 보면 좋을듯 합니다.

꼭!! 알아두기

공공기관의 범위(법 제2조제6호)

- 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
- 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
 1. 「국가인권위원회법」 제3조에 따른 국가인권위원회
 2. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
 3. 「지방공기업법」에 따른 지방공사 및 지방공단
 4. 특별법에 의하여 설립된 특수법인
 5. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교
- 단, 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따름(「개인정보 보호법」 제33조 제7항)

개인정보파일 및 개인정보처리시스템 정의

• 개인정보파일

- (정의) 개인정보파일은 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다. 개인정보파일은 데이터베이스 등 전자적인 형태뿐만 아니라 수기(手記)문서 자료도 포함하지만, 영향평가의 대상이 되는 개인정보파일은 전자적으로 처리할 수 있는 것에 한정되어 있으므로 일반적으로 종이 등의 문서에 수기로 기록된 개인정보 문서는 대상에서 제외된다. 단, 종이로 기록된 개인정보 문서가 PDF 등의 전자적인 매체로 변환될 경우 해당 PDF 파일 등은 평가의 대상이 될 수 있다.

• 개인정보 처리시스템

- (정의) 개인정보처리시스템이란 데이터베이스 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다. 개인정보처리시스템은 일반적으로 데이터베이스(DB) 내의 데이터에 접근할 수 있도록 해주는 응용시스템을 의미하며 데이터베이스를 구축하거나 운영하는데 필요한 시스템을 말한다. 다만, 개인정보처리시스템은 개인정보처리자의 개인정보 처리방법, 시스템 구성 및 운영환경 등에 따라 달라질 수 있으며 작게는 한 대의 서버에서부터 크게는 수백 대의 서버 및 DBMS를 운영하는 것까지 다양한 규모를 가지고 있다. 영향평가에서는 개인정보처리시스템 내의 개인정보파일을 안전하게 보호하기 위하여 필요한 기술적·관리적 및 물리적 안전조치가 적절하게 적용되었는지 여부를 비롯하여 개인정보의 수집, 저장, 이용, 제공, 파기 등 생명주기 상에 관련 법규를 준수하고 정보주체의 권리를 제대로 보장하고 있는지를 확인하고 문제점이 있는 경우 개선방안을 제시하게 된다.

개인정보파일의 운용체계 변경 예시

- 기 수집된 개인정보파일의 처리절차가 변경되는 경우는 개인정보 처리시스템의 추가변경 또는 개인정보 수집경로, 처리절차의 확대·변경하는 경우로 구분
 - 개인정보처리시스템을 추가변경하려는 경우 : 데이터베이스시스템 혹은 응용프로그램 등의 개인정보 처리시스템이 노후하여 이를 신규로 구축하거나 기능을 고도화 하는 경우
 - ※ 예) 교육청이 해당관할 내 학교소속 학생들의 진로상담을 위해 기존에 운용하던 정보 시스템을 신규로 구축하는 경우
 - 개인정보 수집 경로 및 처리절차를 확대·변경하려는 경우 : 기존 개인정보파일의 수집경로가 온라인에서 오프라인까지 확대 되거나, 수집·보유·이용·제공 파기 등 개인정보 처리절차가 변경되는 경우
 - ※ 예) ○○증명서 발급을 위한 개인정보 수집을 기존 각 구청에서 전국 읍·면사무소(주민센터)로 확대하는 경우
- 기관 내부의 다른 정보시스템과 개인정보처리시스템을 새롭게 연계하거나, 기존 연계방식 또는 연계하는 데이터를 변경하는 경우
- 개인정보의 수집 방법을 기존 정보주체로부터 직접 수집하는 방식에서 간접 수집 방식으로 변경하는 경우
- 수집·처리되는 개인정보의 항목이 추가되거나 변경된 경우 또는 개인정보 수집·이용 목적에 변경이 발생하는 경우
- 기존 정보시스템에 신기술을 적용하는 등의 새로운 활용법을 채택함으로써 기존에 수집되거나 향후 수집될 정보가 본인 확인이 가능한 형태로 변경되는 등 시스템 상에 중대한 변화가 발생하는 경우
- 신규 또는 추가로 구축된 시스템이 개인정보 DB에 대한 접근을 관리 또는 통제하기 위해 사용되는 보안체계에 중대한 변화를 초래하는 경우
- 사업의 서비스 이용과정에서 생성되는 정보를 기존에 수집한 개인정보와 결합시킴으로써 정보주체의 프라이버시에 영향을 미칠 수 있는 이차적인 정보가 생성되는 경우
 - ※ 기존 업무처리 절차나 개인정보보호 체계의 변경이 없는 단순 노후장비 교체, 운영·유지보수 사업의 경우 영향평가 대상에서 제외할 수 있다.

꼭!! 알아두기

외부기관과의 연계 예시

- 기존에 보유하고 있는 개인정보파일을 외부기관과 연계하는 경우, 새로운 개인정보파일을 연계하는 경우와 기존 연계 절차를 변경하는 경우로 구분
 - 외부기관의 요청 또는 법률 근거에 의해 개인정보파일을 외부기관과 연계·연동 혹은 이관하는 경우
 - ※ 예) 각 시·군청에서 관리하고 있는 학비지원 대상자를 상위기관인 도청에서 추가로 취합·관리하기 위해 학비지원 대상자 현황을 일정주기로 연계하여 자료를 갱신하고자 하는 경우
 - 기존 외부기관과의 개인정보파일 연계·연동 절차를 변경하려는 경우
 - ※ 예) 각 시·군청에서 관리하고 있는 자원봉사자를 상위기관인 도청에서 취합·관리하고 있는데, 취합하는 자원봉사자의 개인정보가 추가되거나, 취합절차가 기존 공문 및 명단 우편발송에서 실시간 시스템 연동으로 변경하려는 경우

꼭! 알아두기

내부 정책자료(예시)

- (조직·체계 자료) 기관별 개인정보 보호지침, 개인정보보호 내부관리계획, 개인정보 처리방침, 개인정보보호업무 관련 직제표, 개인정보보호규정, 정보보안규정 등
- (인적 통제·교육 자료) 개인정보 관련 조직 내 업무분장표 및 직급별 업무 권한 현황, 정보 시스템의 접근권한에 대한 내부규정, 시스템 관리자 및 개인정보취급자에 대한 교육계획, 위탁업체 관리규정 등
- (정보보안 자료) 방화벽 등 침입차단시스템 및 백신프로그램 도입현황, 네트워크 구성도 등

꼭!! 알아두기

사업 설명자료(예시)

- (사업수행자료) 사업추진계획서, 제안요청서, 과제수행계획서, 요구사항 정의서, (기 구축 시) 업무매뉴얼 등
- (외부연계) 위탁계획서, 연계계획서, 인터페이스 정의서, 아키텍처 설계서 등
- (개발 산출물) 시스템 설계서, 요건 정의서, 업무 흐름도, 기능 정의서, ERD(Entity Relationship Diagram), DFD(Data Flow Diagram), 유스케이스 다이어그램(Use Case Diagram), 시퀀스 다이어그램(Sequence Diagram), 테이블 정의서, 화면 설계서, 메뉴 구조도, 아키텍처 설계서, 시스템 구조도 등

사업발주 시 주의사항

- 제안요청서 작성 시 영향평가 대상 시스템의 설계 완료 전에 영향평가를 수행하도록 일정 계획을 제시하여야 하며, 영향평가 개선계획의 반영여부를 감리 또는 테스트 단계에서 확인할 수 있도록 사업 발주 필요
 - 대상 시스템의 설계 완료 전에 영향평가 수행
 - 영향평가 개선계획의 반영여부를 정보시스템 감리 시 확인해야 하므로, 정보시스템 감리 사업발주 시 관련 요건을 포함하여 발주 필요. 단, 감리를 수행하지 않은 경우에는 정보시스템 테스트 단계에서 영향평가 개선계획의 반영여부를 확인
 - 공공기관의 장은 개선사항으로 지적된 부분에 대한 이행 현황을 영향평가서를 제출받은 날로부터 1년 이내에 행정안전부장관에게 제출해야 하므로, 필요시 관련 요구 사항을 제안요청서에 포함
- 시스템 구축 사업의 일부분으로써 영향평가를 포함하여 발주할 경우 영향평가의 독립성을 심각하게 저해 할 수 있으므로, 구축사업과 분리하여 별도의 사업으로 발주 필요
 - 다만 불가피하게 시스템 구축 사업의 일부로 발주하거나 개인정보보호컨설팅 사업의 일부로 발주하는 경우, 영향평가 사업비용은 별도 분리해야 하며 독립성이 훼손되지 않도록 사업 추진 필요
 - 정보시스템 구축사업을 감리한 업체가 동일한 사업에 대한 영향평가 수행은 불가
 - 정보시스템 구축사업을 수행한 사업자가 동일한 사업에 대해서 영향평가 사업을 수행하는 것은 불가
- 대상기관은 제안서 평가 시 투입인력의 인증서 보유 여부 확인 필요
 - 영향평가 사업은 인증서 보유 등 자격요건을 갖춘 인력만 수행 가능
 - 투입인력은 평가기관에 소속되지 않더라도 전체 인력의 50% 미만에 한해 인증서를 보유한 프리랜서나 타사 인력 활용 가능

※ 인증서 보유여부는 www.privacy.go.kr 영향평가 수행인력 조회메뉴에서 인증번호를 사용하여 조회가능

(꼭! 알아두기)

참여자별 역할비교(참고)

- 개인정보 보호책임자, 보안담당관, 정보통신보안담당관의 고유한 역할과 영향평가팀 내에서의 역할

구분	고유 역할	영향평가팀 내 역할
개인정보 보호책임자 (개인정보총 괄관리자)	<ol style="list-style-type: none"> 1. 개인정보 보호 계획의 수립 및 시행 2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제 4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 5. 개인정보 보호 교육 계획의 수립 및 시행 6. 개인정보파일의 보호 및 관리·감독 7. 개인정보 처리방침의 수립·변경 및 시행 8. 개인정보 보호 관련 자료의 관리 9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 	<ul style="list-style-type: none"> • 영향평가 필요성 및 수행 계획의 적절성 검토 • 점검 기준에 개인정보보호 관련 유관 법률·지침 및 기관 내 규정 등이 적절히 반영되었는지 여부 검토 • 개인정보 처리방침의 내용 검토 • 사업 착수 또는 수행 시 개인정보보호 교육의 시행 • 사업완료 후 시스템 사용자에게 대한 개인정보보호 교육계획 수립 • 영향평가 개선계획의 이행 관리 및 반영여부 확인
보안담당관	<ol style="list-style-type: none"> 1. 연도별 보안업무추진계획 수립 및 심사분석(보안관련 주요 성과 및 실적분석) 2. 보안(인원, 시설, 문서, 자재 등) 진단 3. 보안교육에 관한 사항 4. 비밀소유 및 처리인가자 현황조사 5. 보안서약의 집행 6. 통신보안에 관한 업무(음어·악호자재) 7. 출입통제 등 자체 방호계획 수립, 시행 8. 보안업무 기획 및 조정 등 <p>* 국가정보보안기본지침 제5조(정보보안담당관 운영)제4항</p>	<ul style="list-style-type: none"> • 평가팀에 대한 보안관리 요구사항 검토 • 보안서약, 평가팀 업무 공간 보안점검, 문서보안 등 • 평가대상사업에 따라 시스템이 설치될 공간에 대한 물리적인 보안(출입통제, CCTV 등) 요건 검토
정보통신 보안담당관	<ol style="list-style-type: none"> 1. 정보통신 보안활동 계획 수립 2. 정보통신망 신·증설 시 보안대책 수립 3. 정보통신실, 정보통신망 및 정보자료 등의 보안관리 4. 정보통신 보안업무 지도, 감독 및 교육 5. 정보통신 보안사고 조사 및 처리 6. 정보통신시스템의 보안관리 7. 정보통신 보안업무 심사분석 관장 8. 정보통신 보안관련 지침 등 제도 개선 9. 정보통신망 취약성 진단 10. 정보통신시스템의 보안관리 11. 기타 정보통신 보안관련 업무 	<ul style="list-style-type: none"> • 대상사업에서 소요되는 정보시스템(서버, 네트워크, 보안장비 등) 및 관련 정보자산의 보안요건 검토 및 보안취약성(사전)진단 • 응용프로그램 설계 및 개발 시 보안요구사항 검토 • 웹서버 등의 공개서버에 대한 네트워크 보안 요건 검토 • 기타 개인정보의 노출 및 유출 가능성 진단과 이에 따른 보호대책 검토

꼭!! 알아두기

개인정보 생명주기(Life-Cycle)란?

• 개인정보 생명주기(Life-Cycle)란?

- 개인정보를 취득하여 활용하는 단계로써 통상적으로 수집, 보유, 이용·제공, 파기의 4단계로 구분
- (수집) 정보주체의 개인정보를 취득하는 단계로써, 통상적으로 웹사이트 회원 가입, 서면 신청서 작성, 민원 접수 등의 형태를 통해 이루어짐
- (보유) 수집한 개인정보를 보유하는 단계로써, 보유한 개인정보를 안전하게 관리하며 정보주체의 개인정보 열람·정정권리 등을 보장
- (이용·제공) 수집·저장한 개인정보를 업무적인 목적으로 이용하거나 수집한 공공기관 외의 제3의 기관에게 정보를 제공하는 행위
 - ※ 예를 들어, 특정 자격제도를 운영함에 있어 자격검정시험을 주관하는 기관과 자격 제도를 운영하는 기관이 상이한 경우에는 자격검정시험 주관 기관이 합격자 명단을 자격제도 운영기관과 연계하여 제공
- (파기) 수집 및 이용 목적이 달성된 개인정보를 파기하는 행위를 말함
 - ※ 예를 들어, 이용자가 웹사이트 회원을 탈퇴한 경우에는 특정한 사유가 없는 한 회원이 아닌 사람의 정보를 더 이상 보유하고 있을 필요가 없으므로 해당 정보를 파기해야 함

수집 흐름표 양식 설명

※ 수집 흐름표에서 해당 사항이 없는 경우에는 기재하지 않음

- 1) 평가업무명 : 대상사업 중 어떤 업무와 관련하여 개인정보를 처리하는지 기재
- 2) 수집항목 : 수집하는 개인정보 항목을 구체적으로 기재
- 3) 수집경로 : 개인정보 수집방법이 온라인 또는 오프라인 등 해당 개인정보의 취득경로 기재
 - ※ 회원가입을 통한 수집경로는 웹사이트 회원가입, 온라인을 통한 가입, 서면신청서를 통한 오프라인 방식 등으로 구분
 - ※ 정보주체에게 직접 수집하거나 외부기관에 의해 제공받거나 연계하는 방법으로 수집
- 4) 수집대상 : 개인정보를 수집하는 대상인 정보주체의 유형을 기재
 - ※ 예를 들어, 인터넷 회원의 유형이 학생, 학부모 등으로 구분이 된다면 수집 대상도 “인터넷 회원(학생)”, “인터넷 회원(학부모)”으로 나눠서 작성하여 가급적 수집하는 대상 유형을 구체적으로 기재
- 5) 수집주기 : 개인정보를 수집하는 주기를 기재
 - ※ 웹사이트 회원가입의 경우, 상시적으로 수집
 - ※ 외부기관으로부터 주기적으로 제공을 받거나, 대학 입시와 같이 특정 시기에만 수집되는 경우에는 해당 주기를 기재
- 6) 수집담당자 : 개인정보를 수집하는 부서 및 담당자 기재
- 7) 수집근거 : 수집목적에 따른 법률근거 및 사용자 동의획득 여부 기재
 - ※ 법률에 근거한 수집일 경우 법률 조항을 구체적으로 표시

꼭!! 알아두기

보유·이용 흐름표 설명

※ 보유·이용 흐름표에서 해당 사항이 없는 경우에는 기재하지 않음

1) 평가업무명 : 수집 흐름표와 동일

2) 보유 형태 : 수집한 개인정보를 보유하는 장소 및 형태를 기재

※ 수집한 개인정보는 시스템을 통해 DB에 저장하고, 신청서 등은 캐비닛 등에 보관

3) 암호화 항목 : 개인정보 저장 시 암호화하는 개인정보 항목을 기재

※ 수집한 개인정보를 DB에 저장할 때 '보유 시 암호화 항목'에 해당하고, 신청서 등 다른 매체 보유는 암호화 항목에서 제외

※ 일방향 암호화 되어 있는 경우에는 '()' 후 일방향 암호화하였음을 표기

4) 이용 목적 : 개인정보를 이용하는 목적 기재

5) 개인정보취급자 : 수집한 개인정보를 처리하는 부서 및 사용자 기재

6) 이용 방법 : 개인정보취급자가 개인정보를 이용하는 방법 기재

※ 이용 목적 및 취급자 현황은 개인정보 이용 현황에 따라 복수로 기재

꼭!! 알아두기

제공·파기 흐름표 설명

※ 제공·파기 흐름표에서 해당 사항이 없는 경우에는 기재하지 않음

- 1) 평가업무명 : 수집 흐름표와 동일
- 2) 제공 목적 : 개인정보를 제공하는 목적을 상세히 기재
- 3) 제공자 : 개인정보를 제공하는 부서 및 관련 담당자 기재
- 4) 수신자 : 개인정보를 제공받는 타 기관, 시스템명 기재
- 5) 제공 정보 : 제공하는 상세 개인정보 항목을 기재
- 6) 제공 방법 : 개인정보 제공 시 타 기관에 제공하는 방식 및 시스템 연계 시 연계 방식 기재
- 7) 제공 주기 : 제공하는 개인정보 주기를 기재
- 8) 암호화 여부 : 정보 제공 시 제공 정보 암호화 여부 및 전송 시 암호화 여부 기재

※ 해당사항이 없는 경우에는 기재하지 않음

- 9) 제공 근거 : 개인정보를 제공하는 법적 근거 및 사유 기재

※ 법률에 근거한 제공일 경우 법률 조항을 구체적으로 표시

- 10) 보유기간 : 개인정보를 수집한 후 파기하기 전까지의 보관기간 명시

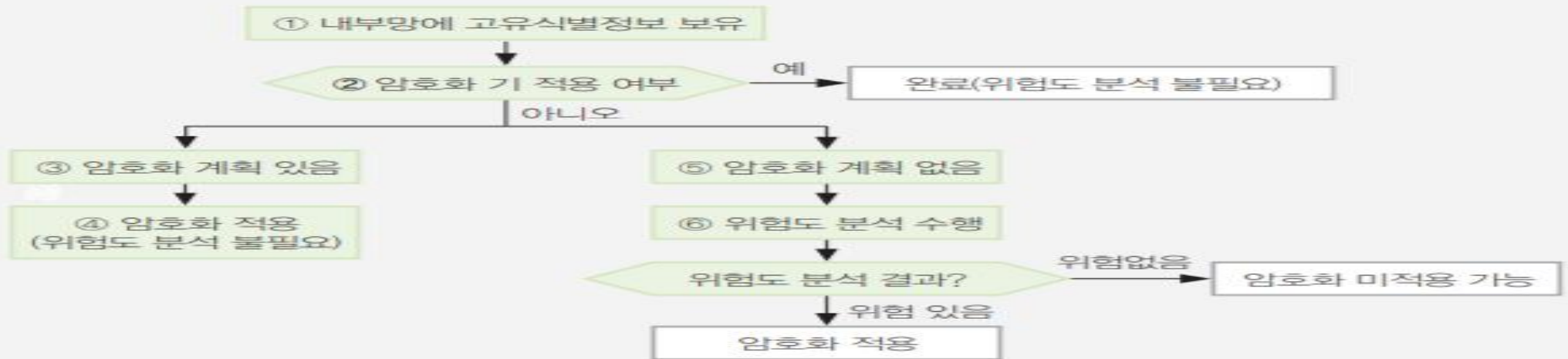
※ 보관기간은 정확한 기한이 있을 경우, 1년, 10년과 같이 표기하고, 정확한 기한이 없을 경우, '웹사이트 회원 탈퇴 시까지' 등과 같이 보유 기간 산정 원칙을 명시

- 11) 파기담당자 : 개인정보를 파기하는 부서 및 담당자
- 12) 파기 절차 : 파기가 결정된 개인정보에 대해 파기주기와 파기방법 기재
- 13) 분리 보관 여부 : 법령 등에 따라 개인정보를 파기하지 않고 보관하는 경우, 보존DB 등을 구성하여 다른 개인정보와 분리 저장·관리하는지 기재 (개인정보 보호법 제21조제3항 참조)

꼭!! 알아두기

고유식별정보 암호화 적용여부 판단 절차

- 고유식별정보는 「개인정보 보호법」 제24조, 제29조 및 「개인정보의 안전성 확보조치 기준」 고시에 따라 암호화 적용 필요
- 단 내부망에 고유식별정보(주민등록번호 제외)를 저장하는 경우, 「위험도 분석」 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행 가능



- ① 외부망 또는 DMZ에 고유식별정보를 저장할 경우 필수적으로 암호화를 적용하여야 함. 다만 내부망에 고유식별정보를 저장할 경우 영향평가 또는 위험도 분석에 근거하여 암호화 적용 여부 및 적용범위를 결정 가능
- ② 내부망에 저장된 고유식별정보가 암호화 되어 있지 않을 경우 암호화 계획 수립 여부 검토
- ③ 암호화 계획이 수립되어 있을 경우 별도 위험도 분석 실시 불필요
- ④ 암호화 계획에 따라 암호화 적용
- ⑤ 암호화 계획이 없을 경우 위험도 분석 수행 필요하며, 영향평가에 포함하여 수행하거나 공공기관 자체적으로 수행 가능
- ⑥ 「개인정보 위험도 분석기준」에 따라 위험도 분석 수행 후 고유식별정보에 대한 암호화 적용 여부 최종 결정
 - ※ '개인정보 위험도 분석 기준 및 해설서' 참고
 - ※ 단, 주민등록번호는 위험도 분석 결과와 상관없이 암호화 (시행령 제21조의2 참조)

개인정보 처리 업무표 양식 설명

1) 평가업무명

- 영향평가 대상시스템에서 개인정보가 처리되는 업무를 주요 업무단위로 기재
 - ※ 개인정보에 대한 관리가 가능한 범위로 유사한 업무단위로 묶어 단위업무를 구성
 - ※ 평가업무를 너무 포괄적으로 분류할 경우 평가가 부실하게 수행될 가능성이 있으므로, 중요하거나 복잡한 업무는 세분화하여 분류함으로써 평가의 구체성을 높일 필요가 있음

2) 처리 목적

- 업무에서 개인정보를 처리하는 목적 및 사유를 기재
 - ※ 개인정보처리방침이나 개인정보 수집 및 이용 동의 절차에 명시된 '개인정보의 수집·이용 목적'을 참고하여 조사 가능

3) 처리 개인정보

- 영향평가의 평가업무 단위로 처리되는 개인정보 항목 기재
 - ※ 주소, 수급자주소, 자택주소, 자택번지 등과 같이 유사한 항목이 있는 경우에도 '주소'로 대표화하지 않고, 가급적 구분하여 상세히 기재(단, 명칭만 다르고 의미가 같은 경우에는 용어를 1개로 통일하여 기재)
- 개인정보 항목 기재 시 업무처리를 위해 필수 정보인지 선택정보인지 여부를 명확히 알 수 있도록 '필수', '선택' 항목 구분 표기

4) 주관부서

- 해당 개인정보 처리 업무를 주관하는 부서명 기재
 - ※ 여러 부서가 공동으로 주관할 경우 모두 기재

5) 개인정보 건수

- 처리되는 개인정보 건수 기재
 - ※ 여러 개인정보가 혼재하여 건수가 상이한 경우, 가장 많은 정보를 기준으로 기재하며, 고유식별정보가 포함된 경우, 건수 뒤에 ‘()’ 후 고유식별정보의 개수를 추가 기재
 - ※ 동일한 정보주체에 대한 정보가 중복되어 존재할 경우, 중복을 제거한 건수 기재
 - ※ 신규 사업의 경우, 향후 1년 내에 예상되는 건수를 입력

6) 개인정보 영향도

- 처리 개인정보의 중요도에 따라 영향도를 산정
 - ※ 대상사업(대상시스템)의 개인정보 처리업무, 처리되는 개인정보현황, 개인정보 항목의 조합수준에 따라 영향도를 산정하고, 자산(평가업무) 가치를 측정하여 ‘개인정보 영향도’를 작성

평가업무명	처리목적	처리 개인정보	주관부서	개인정보 건수	개인정보영향도
...
회원가입	본인확인	생년월일	○○사업부	10만	3
	본인확인	이메일주소	○○사업부	10만	3

상담업무	본인확인	성명	○○사업부	5천	3
	본인확인	생년월일	○○사업부	5천	3

실업급여 관리	사용자 인증	비밀번호	○○사업부	3만	5
	실업급여 입금	계좌번호	○○사업부	3만	5
...

- ※ 업무단위(평가업무명)별로 처리 개인정보를 그룹핑하여 하나의 셀에 정리하고 해당업무에서 처리하는 개인 정보의 영향도 중 가장 높은 숫자를 입력 (아래 “개인정보 처리업무표 예시” 참고)

PIA 개인정보 영향평가 개념잡기

◇영향평가 인증 대상 딱 2 가지만 생각하자.◇

1.공공 기관 !!!!

2.개인정보파일 보유건수 중 5 단위로 암기해보자

♥ 5만-5만명이상 민감정보

♥ 50만-50만명 의 연계 가능한 개인정보

♥ 100만 – 100만명이상 개인정보

이것만 기억하자.

- 수고 하셨습니다. ^^

많이 부족한 자료 이지만, 나름대로 열심히 공부 하였고, 지금 이시간에도 열심히 공부할 누군가와 공유 하고 싶어 작성 하게 되었습니다.

감사합니다 ^^

- 무료, 공개 스터디 카페 입니다.
- 배포 자유!! 하지만 수정은 금지 합니다. !! (힘들게 제작한 제작자 입니다)
- 비영리 목적으로 순수 하게 학습이 목표 입니다.
- 순수한 학습 목적 이기에 검색 엔진에서 검색이 되던 안되던, 신경 쓰고 있지 않습니다.
- 그렇기 때문에, 학습 하며 작성한 자료를 이미지 그대로 첨부 하였습니다.
- 순수한 학습 목적 이기에 검색 엔진에서 검색이 되던 안되던, 신경 쓰고 있지 않습니다.
- 잘못된 부분이나, 수정될 부분이 있으면 피드백 주시는되로 즉시 수정 하도록 노력하겠습니다.
- KISA, google, Naver 사의 위키피디아, 이미지 를 사용 하였습니다. 문제시, 즉시 삭제 하도록 하겠습니다.