개인정보 영향평가
- 공공기관 -

2017. 6

KISA 한국인터넷진흥원

1. 영향평가 정의

법적 정의 (개인정보보호법 제33조)

- 개인정보파일의 운용으로 인하여 **정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가**(이하 " 영향평가 " 라 한다)를 하고 그 결과를 행정자치부장관에게 제출하여야 한다.

일반적 정의 : 개인정보 영향평가(PIA : Privacy Impact Assessment)란?

- 개인정보파일을 운용하는 개인정보처리 시스템을
  1) **신규 도입**하거나
  2) **기존에 운영중인 개인정보 처리시스템의 중대한 변경 시**

- 개인정보 처리시스템의 구축 · 운영 · 변경 등이 **개인정보에 미치는 영향(impact)**을

- **사전에 조사 · 예측 · 검토**하여 **개선방안을 도출**하는 체계적인 절차

KISA

2. 영향평가 목적

목적

개인정보를 취급하는 정보시스템에 대해 영향평가를 실시하여
사전에 개인정보 침해 요인을 파악하고
개선방안을 수립 · 적용하여 **침해사고를 사전예방**

기대효과

- 개인정보 법제도에 대한 이해 제고
- 개인정보 보호체계 확립
- 개인정보보호 관련 규제 준수 이행
- 침해요인에 대한 보완 및 개선

효과적인 영향평가가 되려면?

1. 정확한 현황파악을 위해 영향평가업체의 자료요구에 최대한 협조
2. 최대한 구체적인 개선방안 마련을 요구(관련 기술, 솔루션비교, 필요예산, 기대효과 등)

KISA

3. 영향평가 수행시기

개인정보를 수집·이용하려는 대상기관은
정보시스템 구축·변경시 BPR/ISP(또는 분석·설계)단계에서 영향평가를 수행하여야 한다.

▶ **현재 운영중인 기 구축 시스템은 2016.9.30 까지 영향평가 수행 완료**(시행령 부칙 제6조(개인정보 영향평가에 관한 경과조치))

4. 영향평가 수행대상

개인정보 보호법 시행령 제35조(개인정보 영향평가의 대상)

- 전자적으로 처리할 수 있는 개인정보파일

1. **5만 명** 이상의 **민감정보 또는 고유식별정보**가 포함된 개인정보파일
2. 공공기관 내부 또는 외부 개인정보파일과 **연계 결과 50만 명** 이상의 개인정보가 포함된 개인정보파일
3. **100만 명** 이상의 개인정보가 포함된 개인정보파일
4. 개인정보 검색체계 등 기존 개인정보파일의 운용체계를 변경하는 경우, **변경된 부분**

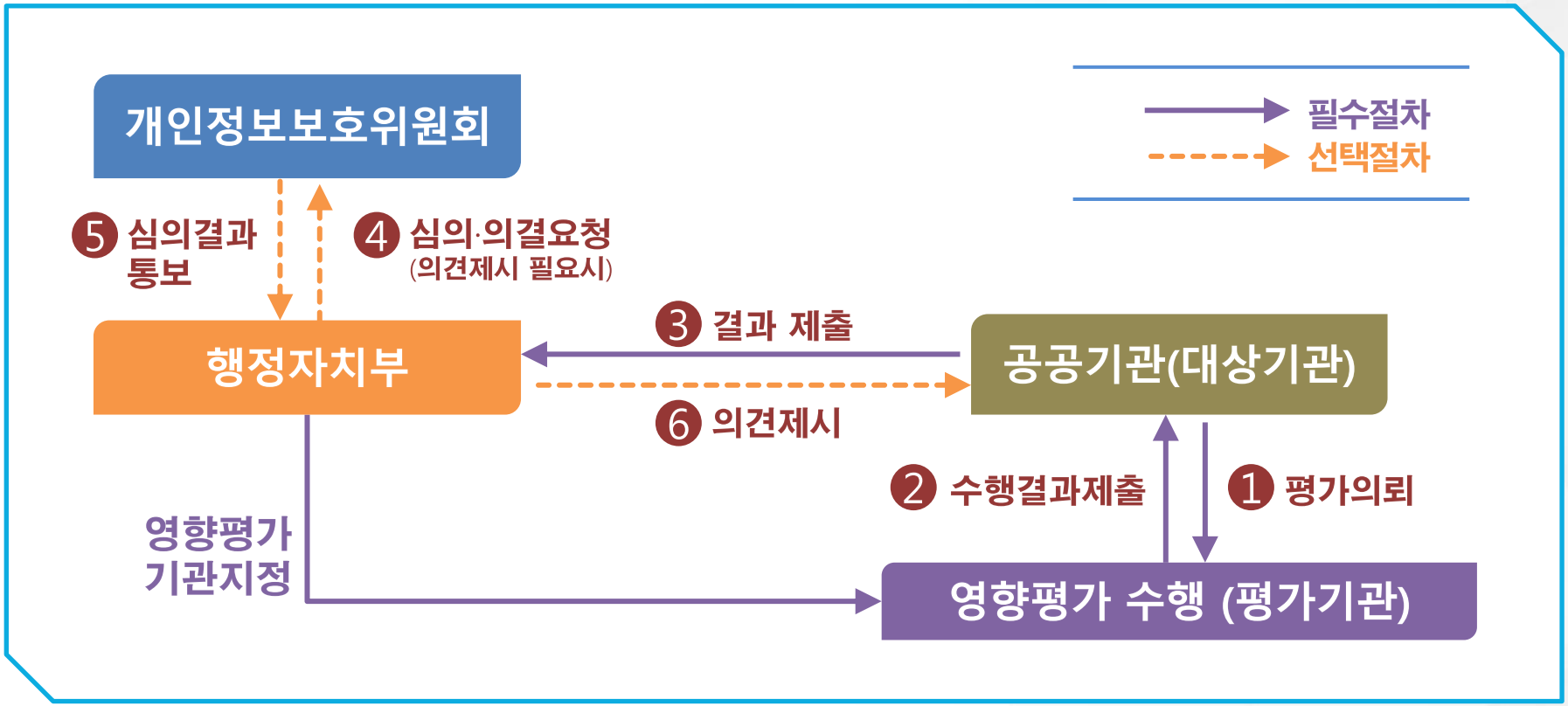
※ 신규 개인정보파일의 경우 정보주체의 수를 합리적으로 추정하여 수행대상 여부 결정

※ 현재는 조건에 해당하지 않지만 가까운 시일에 조건에 해당될 것으로 예상되는 경우 영향평가 수행

KISA

5. 영향평가 수행 체계

- **공공기관은 영향평가 대상 시스템에 대해서는 행정자치부에서 지정한** 개인정보 영향평가기관에 의뢰하여 평가를 수행**하고 그 결과를 행정자치부에게 제출한다.**
- **행정자치부는** 개인정보보호위원회의 심의·의결을 거쳐 해당 사업에 대한 의견 제시가능



6. 영향평가 기관

- **평가기관 지정** : 2017**년 현재** 총 18개 기관 지정/지정갱신

보안전문업체	10개	감리업체	7개	SI업체	1개

2017년 지정갱신기관 (17.1.23)

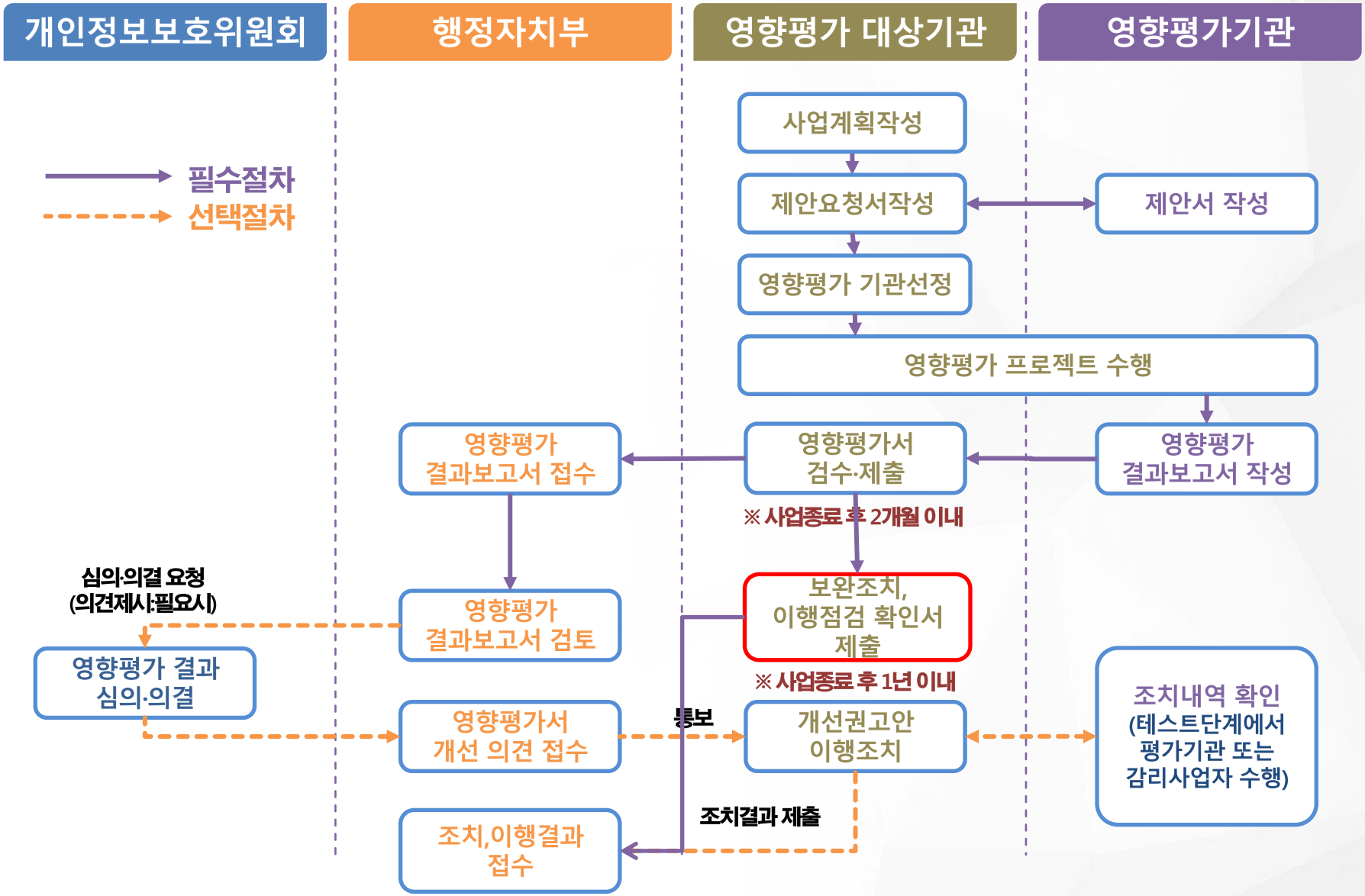
기관명	비고
A3 시큐리티	보안
케이씨에이	감리
LG CNS	SI
소만사	보안
시큐베이스	보안
싸이버원	보안
키삭	감리
한국IT컨설팅	감리
한국정보기술단	감리

기관명	비고
대진정보통신	보안
씨드젠	보안
에스에스알	보안
에이스솔루션	감리
한국전산감리원	감리
씨에이에스	감리
SK인포섹	보안
안랩	보안
이글루시큐리티	보안

※ **영향평가기관 지정심사위원회 심사를 거쳐 평가기관 신규지정 및 지정갱신**

KISA

7. 영향평가 수행 절차


개인정보보호위원회
행정자치부
영향평가 대상기관
영향평가기관
필수절차
선택절차
사업계획작성
제안요청서작성
제안서 작성
영향평가 기관선정
영향평가 프로젝트 수행
영향평가 결과보고서 접수
영향평가서 검수·제출
영향평가 결과보고서 작성
※ 사업종료 후 2개월 이내
심의·의결 요청
(의견제시:필요시)
영향평가 결과보고서 검토
보완조치, 이행점검 확인서 제출
※ 사업종료 후 1년 이내
영향평가 결과 심의·의결
영향평가서 개선 의견 접수
통보
개선권고안 이행조치
조치내역 확인
(테스트단계에서 평가기관 또는 감리사업자 수행)
조치결과 제출
조치,이행결과 접수

8. 영향평가 점검 항목


1. 대상기관
개인정보보호 관리체계
2. 대상시스템의
개인정보보호 관리체계
3. 개인정보 처리단계별
보호조치
4. 대상시스템의
기술적 보호조치
5. 특정IT기술 활용시
개인정보보호
5개 영역
78개 점검항목
(기관,시스템의 특성에 따라 점검항목 가감)

8. 영향평가 점검 항목

1. 대상기관 개인정보보호 관리체계	2. 대상시스템의 개인정보보호 관리체계	3. 개인정보 처리단계별 보호조치	4. 대상시스템의 기술적 보호조치	5. 특정IT기술 활용시 개인정보보호

평가분야

개인정보보호 조직, 개인정보보호 계획, 개인정보 침해대응, 정보주체 권리보장

주요결함

- *개인정보 내부관리계획서에 재해,재난 대비 안전조치 사항 등 필수항목 누락*
- *개인정보보호책임자 연1회 이상 내부관리계획 이행 점검 미흡*
- *개인정보 침해대응 모의훈련 미 실시 (훈련계획서, 결과서 없음)*
- *정보주체 권리행사 방법 안내 미흡 (열람,정정,삭제 신청서 미비)*

8. 영향평가 점검 항목

평가분야

개인정보취급자 관리, 개인정보파일 관리, 개인정보 처리방침

주요결함

- *개인정보취급자 계정 관리 미흡 (직무변경시 계정권한 변경 지연)*
- *개인정보파일 등록 누락*
- *개인정보파일 1개당 1개의 대장 작성 안됨*
- *개인정보보호 교육 미 이수자에 대하여 추가 교육 미 실시*
- *개인정보처리방침에 변경이력 안내 미흡*

8. 영향평가 점검 항목

평가분야

개인정보 수집, 보유, 이용/제공, 위탁, 파기

주요결함

- *개인정보 수집 동의서 누락 (이벤트 등 법령에서 정한 소관업무가 아닌 경우)*
- *온라인에서 수집시 동의함에 이미 체크가 되어 있는 경우*
- *개인정보 "목적외이용 및 제3자제공" 대장에 일부 제공내역의 누락*
- *개인정보 목적외이용 및 제3자제공 후 홈페이지에 제공사실 미 공개(30일 이내, 10일)*
- *위탁업체 일부를 홈페이지에 미 공개*
- *수탁자에 대하여 안전조치 사항 교육, 현황 점검 등 관리감독 미 실시*
- *개인정보 분리보관 미흡*

8. 영향평가 점검 항목

1. 대상기관 개인정보보호 관리체계	2. 대상시스템의 개인정보보호 관리체계	3. 개인정보 처리단계별 보호조치	**4. 대상시스템의 기술적 보호조치**	5. 특정IT기술 활용시 개인정보보호

평가분야

접근권한 관리, 접근통제, 개인정보의 암호화, 접속기록의 보관 및 점검, 악성프로그램 방지, 물리적 접근방지, 개인정보의 파기, 기타 기술적보호조치, 개인정보처리구역 보호

주요결함

- *개인정보취급자 공용ID 사용*
- *대량의 개인정보취급자 또는 관리자가 일반 ID,PW 방식의 인증사용*
- *로그인 실패횟수 제한, 세션 타임아웃 적용 미흡*
- *접근권한 변경 이력 보관 미흡 (최소 3년 이상)*
- *인터넷 홈페이지를 통한 개인정보/파일 노출 여부 점검 미흡*
- *메일전송, 보조저장매체에 고유식별정보 전달시 암호화 미 실시*
- *개인정보처리시스템 접속로그를 동일시스템에 보관*

KISA

8. 영향평가 점검 항목

평가분야

CCTV, RFID, 바이오정보, 위치정보

주요결함

- *CCTV 운영위탁시 안내판에 수탁사 명칭, 연락처 표시 누락*
- *"영상정보처리기기 운영관리 방침"의 영상정보 보관기간과 실제 보관기간 상이*
- *개인정보가 포함된 RFID 카드 발급시 통지 및 안내 누락*
- *RFID 카드에 태그부착사실, 기록되는정보, 관리책임자 연락처 등 표시 미흡*
- *바이오정보 수집시 원본정보와 신상정보를 분리보관 하지 않음*

9. 영향평가 FAQ

Q 우리 시스템의 자체 보유수는 30만명이고 다른 시스템의 100만명 개인정보를 조회하여 우리시스템에서 볼수 있다면 영향평가 대상인가요?

A 단순 조회는 연계로 보지 않습니다. 그러므로 연계결과 50만명 이상에 해당하지 않기에 영향평가 대상이 아닙니다.

Q 영향평가는 기관 단위로 수행해야 하나요? 시스템 단위로 수행해야 하나요?

A 시스템 단위로 수행할 수도 있지만 통합하여 기관단위로 수행하는 것을 권고합니다.

KISA

9. 영향평가 FAQ

Q 영향평가 이행점검 결과는 언제까지 제출해야 하나요? 또한 모든 항목을 조치 완료 해야 하나요?

A 영향평가 후 1년 이내 제출해야 합니다. 결함조치는 기간이 오래걸리는 경우 해당사유와 기간을 명시하되 법적 요구사항은 반드시 조치해야 합니다.

Q 영향평가를 받지 않으면 어떻게 되나요?

A 개인정보 침해위험요소를 파악하지 못해 사고위험이 커지고, 사고발생시 가중 처벌이 될수 있으며, 공공기관 관리수준진단에서 감점을 받게 됩니다. 또한 행정자치부 및 상급부처의 개인정보보호 실태점검시 주의를 받게 됩니다.

참고

영향평가 수행주체 등

- 개인정보 파일에 대해서 **소유권을 가지고** 있거나, 해당 개인정보파일에 대한 **관리(수정·변경, 조회, 파기 등) 권한을 가지고** 있는 기관에서 영향평가 수행
- 개인정보 파일을 운용하고 있는 **개인정보 처리시스템을 소유하거나 운영관리 권한을 가지고** 있는 기관에서 영향평가를 수행
- 영향평가 대상인 **물리적 장비, 응용프로그램 또는 개인정보파일이 중앙행정기관과 지자체 등에 분산 위치하는 경우, 지자체 등은 중앙행정기관으로 부터 영향평가 수행 범위 등에 대한 지침을 받아 영향평가 수행**

개인정보 영향평가 관련 자료

- 개인정보 영향평가 수행 관련 자료는 "개인정보보호 종합포탈" www.privacy.go.kr 에서

  사업자 > 개인정보영향평가 > 자료실 에서 확인 가능

KISA

맺음말

개인정보 영향평가는
개인정보 건강검진 !!

Internet On, Security In!

감사합니다