2019년

개인정보 보호법 위반사례 및 대응방안(1)

믿을 수 있는 개인정보 활용, 신뢰사회의 기본입니다

Privacy by Trust, Trust by Privacy

강사 : 충북대학교 신동혁 교수

행정안전부

KISA
Korea Internet & Security Agency

Contents

Ⅰ. 개인정보 실태조사

조직의 개인정보보호 문제

개인정보 유출사고

행정처분(과태료),
형사처벌,
민사

내부자 유출(실수, 고의),
해킹

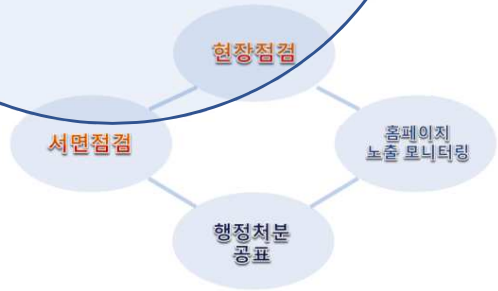
知彼知己　他山之石

개인정보
노출점검

실태점검

개인정보 실태점검

행정처분(과태료),
형사처벌



(사전예방) 행정기관 기준
(사후관리)개인정보유출, 민원인 신고

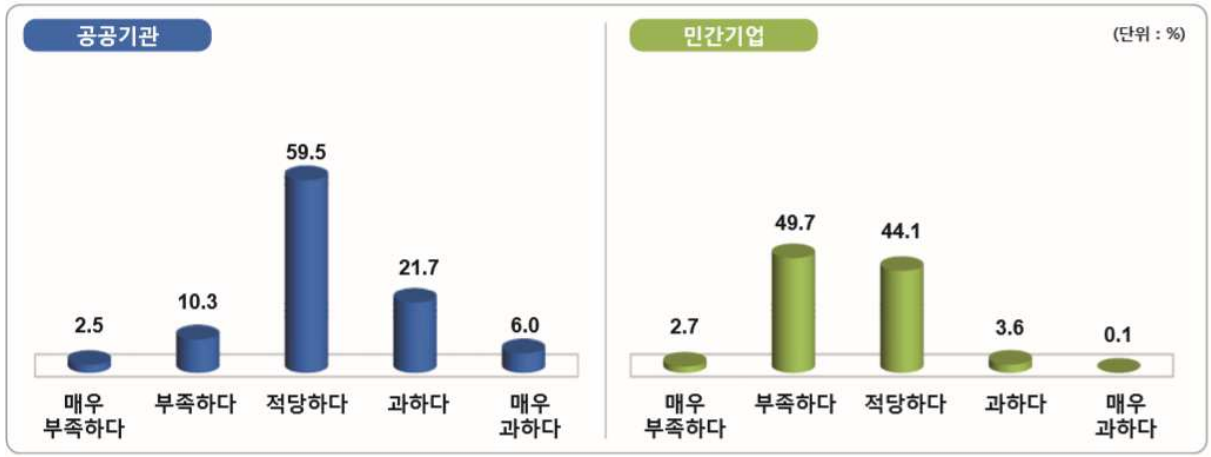
개인정보 유출사고

개인정보 침해시 피해구제 관련 정보주체 대응

구 분		어떠한 대응도 하지 않음	사업자 상대 민원제기 등	수사 기관에 신고 또는 고발	소송 제기	정부 지자체에 신고/민원 제기	개인정보 침해신고 센터 등에 신고	개인정보 분쟁 조정 신청	기타
전 체		67.4	13.7	7.9	7.8	6.3	5.8	3.9	1.9
성별	남성	63.8	17.2	8.1	10.1	7.1	6.5	4.6	1.1
	여성	70.8	10.3	7.7	5.7	5.5	5.1	3.2	2.6
연령	10대	69.4	10.5	10.9	3.4	9.8	6.9	4.7	3.8
	20대	70.7	11.5	8.4	6.4	6.8	11	4.7	3.3
	30대	67.5	14.5	8.5	9.3	6	2.6	3.7	2.1
	40대	68.3	13.3	6.1	9	6.4	5.4	2.5	0.2
	50대	67.3	13	8	10.3	5.3	4.9	3.2	–
	60대 이상	61.5	18.5	6.4	7.2	4.3	4.7	4.7	2.6

[출처 : 2015년 개인정보 보호 실태조사]

개인정보 유출사고 발생시 처벌 강도



홈페이지 개인정보 노출 모니터링

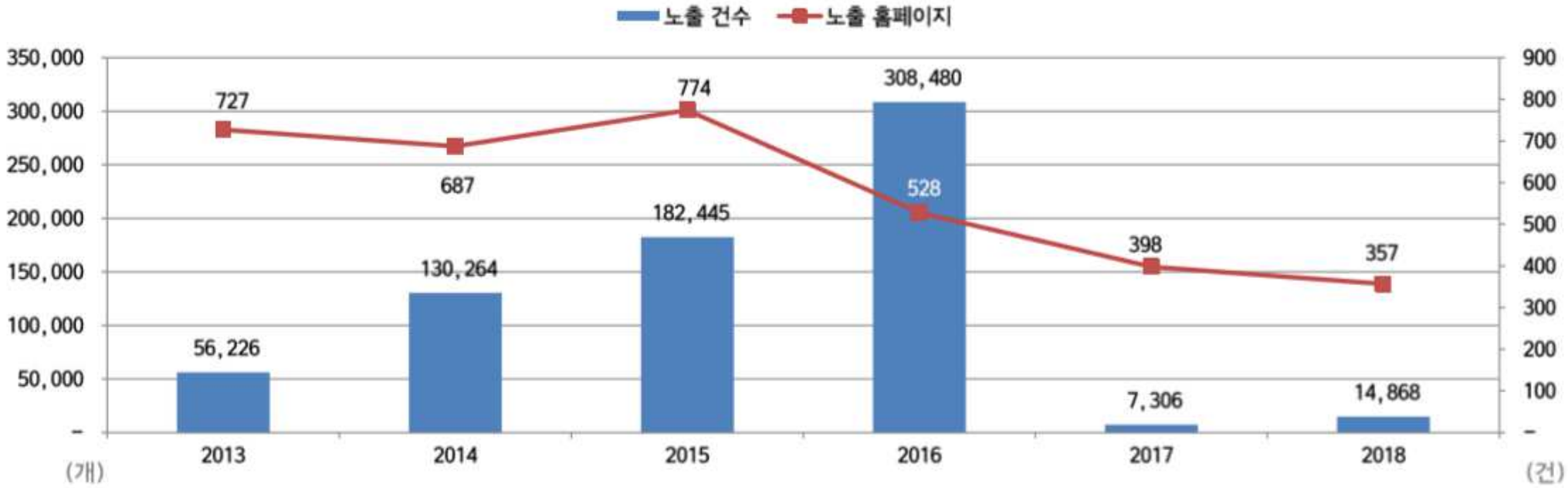
구 분	점검 홈페이지 수	노출 홈페이지 수	기관별 개인정보 노출 건수				
			합계	중앙 부처	지자체	산하 기관 등	비영리·협회
2012년	1,620,052	1,164	35,595	2,047	5,720	19,058	8,770
2013년	2,620,714	727	56,226	1,048	18,863	20,723	15,592
2014년	3,448,580	687	130,264	1,629	26,045	15,394	87,196
2015년	4,184,428	774	182,445	509	6,623	32,903	142,410
2016년	4,634,890	528	308,480	365	15,066	6,385	286,664
2017년	4,911,246	398	7,306	261	1,993	824	4,228

구 분		2012년	2013년	2014년	2015년	2016년	2017년
주민등록번호	사이트 수	1,055	667	604	595	452	341
	노출 건수	33,738	55,939	125,907	157,092	286,922	6,673
여권번호	사이트 수	5	3	17	126	48	46
	노출 건수	14	52	647	23,821	21,234	350
외국인등록번호	사이트 수	74	52	23	28	13	16
	노출 건수	1,733	226	316	1,471	220	272
운전면허번호	사이트 수	31	5	43	25	15	7
	노출 건수	297	9	3,394	61	104	11

개인정보 노출점검

공공기관 홈페이지 개인정보 노출 현황(최근 6년간)

(자료: 한국인터넷진흥원)



[검색정보] - "고유식별정보" 4종
①주민등록번호 ②여권번호 ③외국인등록번호 ④운전면허번호

공공기관 홈페이지_개인정보 노출 경향

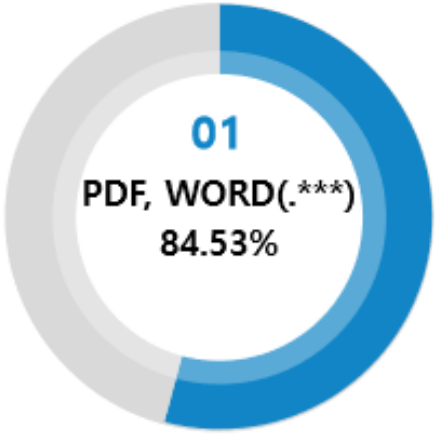
- 최근 6년간 개인정보 노출 홈페이지 수는 50.9% 정도 감소했다. 노출 건수는 16년도 까지 지속적 증가 추세를 보였다. 17년 노출 건수가 급격히 감소 했지만, 18년 노출 건수가 작년에 비해 두배 정도 늘었다.
- 노출 홈페이지는 작년보다 모니터링 대상이 2만 여개가 감소 했고, 노출 건수는 작년 OO시청 사이트에서 약 7천 건의 개인정보가 대량 노출되 작년대비 2배로 증가 하였다.

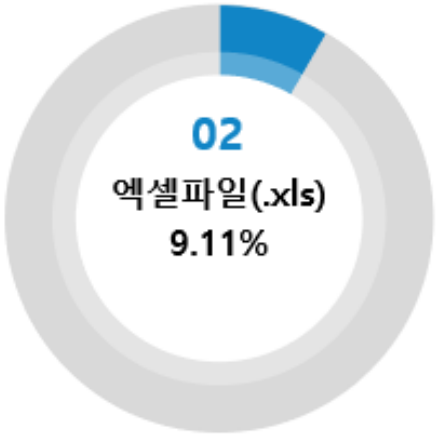
공공기관 홈페이지 개인정보 노출 형태

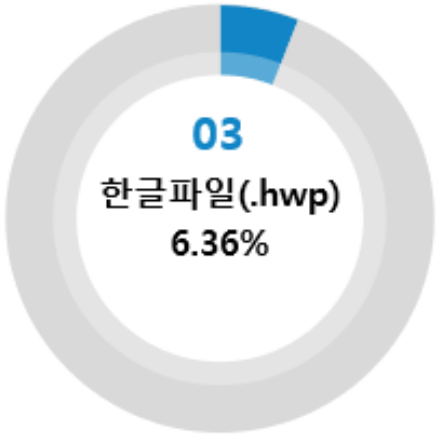
대분류	중분류	주요 노출 형태	노출원인
공공기관	중앙행정기관	- 참여마당 '자유게시판' 글에서 주민등록번호 노출 - 정보조회의 '일반정보' 글에서 운전면허번호 노출	게시글 노출
		- 합격자발표 게시판의 'OO시험합격자 명당' 첨부파일에서 여권번호 노출 - 임대안내 게시판의 신청서류 첨부파일에서 주민등록번호 노출 - 시험공고/공지사항 게시판의 '공채 임용유예자 명단' 첨부파일에서 주민등록번호 노출	첨부파일 노출
	지방자치단체	- '개별공시지가 이의신청' 첨부파일에서 주민등록번호 노출 - 과제검색 게시판의 첨부파일에서 주민등록번호와 외국인등록번호 노출	첨부파일 노출
		- 정보공개창 게시판의 '배출업소현황' 첨부파일에서 주민등록번호 노출 - 우리동소식 게시판의 '알선대상자 명단' 첨부파일에서 주민등록번호 노출 - 'OO시 선수명단' 파일에서 주민등록번호 노출 - 행정처분 명령서 파일에서 주민등록번호 노출	첨부파일 노출
	초중고	- '급식행정공개', '가정통신문'에서 주민등록번호 노출 - 행정실 게시판의 '운영위원회' 파일에서 주민등록번호 노출 - 부별업무자료의 '스카우트' 알집파일 내에 존재하는 첨부파일에서 주민등록번호 노출	첨부파일 노출
		- 민원센터의 '학사/학적변동' 글에서 주민등록번호 노출 - 사이버강좌의 '개설강좌' 글에서 주민등록번호 노출	게시글 노출
	대학교	- '어학원 수강신청' 파일에서 외국인등록번호 노출 - 행정실 공지사항 게시판의 첨부파일에서 주민등록번호와 외국인증록번호 노출	첨부파일 노출
		- OO대학교 관리자페이지에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡

개인정보 노출점검

2018년 첨부파일 노출 유형 Top 3







엑셀

- Sheet 숨기기 처리
- 함수 치환 처리
- 행/열 숨기기
- Sheet 보호 처리
- 글자색을 배경색과 같게 처리
- 메모에 "개인정보" 입력
- "개인정보"가 포함된 개체 삽입 (OLE개체)

한글

- 한글파일 (서식)에서 노출된 "개인정보"

이미지

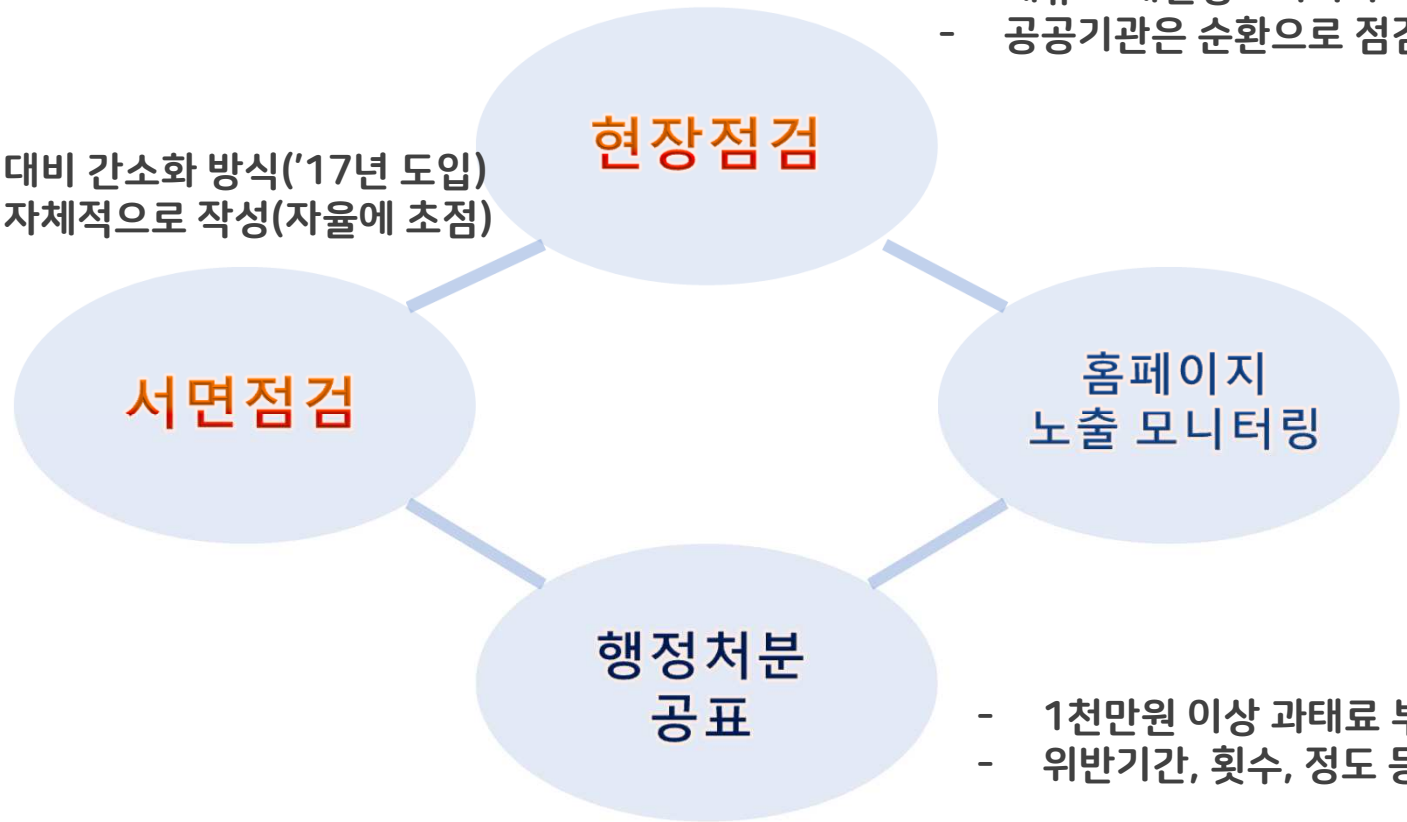
- 이미지 파일에 "개인정보" 포함

편리하게 주어진 "기능"과 "옵션"을 통해 노출이 되고 있음. 그리고 일부 "잘못된 사용"...

개인정보 실태조사

개인정보 실태점검 개요

- 대규모 개인정보처리자 대상
- 공공기관은 순환으로 점검



- 현장점검 대비 간소화 방식('17년 도입)
- 수검기간 자체적으로 작성(자율에 초점)

- 1천만원 이상 과태료 부과 업체
- 위반기간, 횟수, 정도 등을 고려

개인정보 실태조사

연도별 월별 기획점검 분야

점검월	2013년	2014년	2015년	2016년	2017년
1월	렌트카	협회·단체 등	공공기관	보건·복지	산업·물류
2월	-	증권·자산 운용	보건·복지	산업·물류	공공기관
3월	교육 기관 대형 병원	온라인 게임	공공·교육 수탁사	공공기관	시설·문화
4월	TM 업체	대학	교육	의료·통신 수탁사	교육
5월	공공기관	대형 병원	수탁사(정부 합동)	교육	보건·복지
6월	대부업 등	화장품 판매	방송·통신	공공·교육 수탁사	협회·단체 등
7월	대기업	시·군·구청	협회·단체	중개·생활·임대	산업·물류
8월	입시 학원	할부 리스	중개·생활·임대	방송·통신	중개·생활·임대
9월	성형 외과 등	온라인 쇼핑	통신·산업 수탁사	생활·산업 수탁사	공공기관
10월	회원제 업체	교육청	시설·문화	시설·문화	교육
11월	지방 공기업	지방 의료원	공공기관	공공기관	산업·물류
12월	카드 업체	포인트 카드	정보·문화 수탁사	문화·금융 수탁사 산업·물류	보건·복지

개인정보 실태조사

개인정보보호법 항목별 위반사례

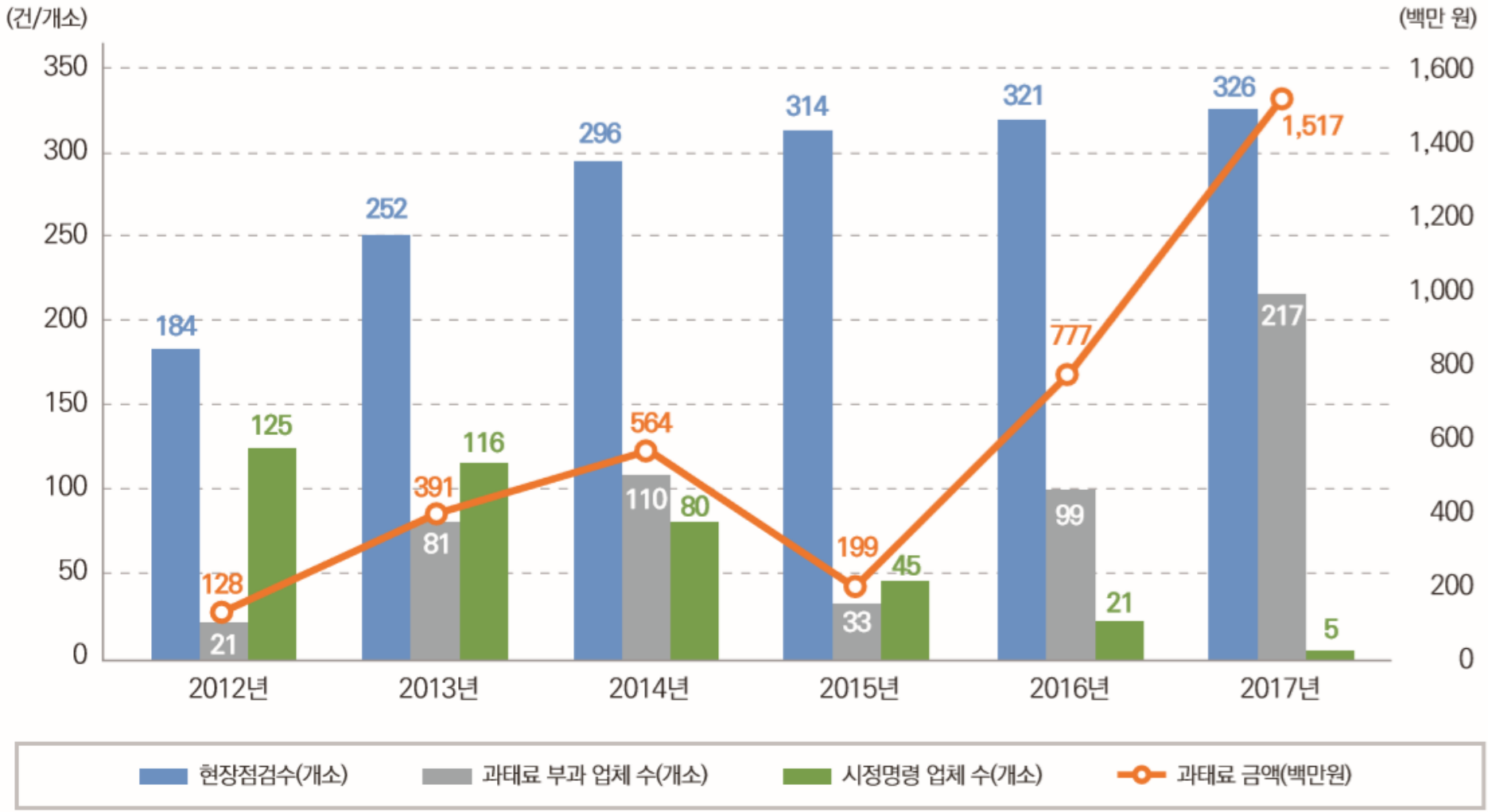
위반 내용별 행정 처분 현황 (단위 : 건)

구 분	계	위반 내용별					
		안전 조치 미흡	CCTV 관리 위반	미동의/ 과도 수집	동의/고지 방법 위반	위·수탁 관리 위반	방침 수립 등 기타
과태료	748	413	33	45	83	85	89
시정조치	661	104	156	65	112	100	124
개선권고	1,026	282	352	143	52	45	152
계	2,435	799	541	253	247	230	365
비율	100%	32.81%	22.22%	10.39%	10.14%	9.45%	14.99%

출처:행정안전부,KISA, 2013~2017 개인정보 실태 점검 및 행정 처분 사례집 2018, 39면.

(2017.1월) : 산업 물류분야 고유식별정보 처리제한 위반 등 관련법 위반 12개사에 과태료 13건 8,000만 원 부과
(2017.2월) : 주민등록번호 암호화 보관 위반 등 관련법 위반 공공기관 24개 기관에 개선권고 15건, 과태료 15건 9,900만 원 부과
(2017.3월) : 문화분야 목적이 달성된 개인정보 미파기 등 관련법 위반 업체 23개사에 개선권고 1건, 과태료 28건 1억 6,000만 원 부과
(2017.4월) : 교육분야 주민등록번호 처리제한 위반 등 관련법 위반 기관 27개 교육기관에 개선권고 8건, 시정명령 2건, 과태료 32건 1억 8,700만 원 부과
(2017.5월) : 보건·복지분야 민감정보 안전성 확보조치 위반 기관 18개 건강검진 의료기관에 대해 과태료 20건 1억 1,400만 원 부과
(2017.6월) : 공공 협회분야 민감정보 안전성 확보조치 위반 등 관련법 위반 기관 14개에 대해 개선권고 16건, 과태료 7건 4,700만 원 부과
(2017.7월) : 산업물류분야 개인정보 수집 시 구분동의 획득 미비 등 관련법 위반 기관 16개 에 대해 과태료 19건 1억 2,500만 원 부과
(2017.8월) : 위탁업무 및 수탁자 미공개 등 관련법 위반 기관 18개 중개·임대·생활분야에 대해 과태료 21건 1억 1,000만 원 부과

2012~2017년 10월 현장점검, 과태료 부과 및 시정명령 추이



행정처분결과 공표제도(50개 기관)

행정 처분 종류 및 요건

종 류	성 격	처분 요건	근거
과태료	법 위반	과태료 부과 대상 규정 위반 시(5천~1천만 원)	§75
과징금	법 위반	주민등록번호 유출 및 안전 조치 위반 시(5억 원 이하)	§34의2
시정조치	법 위반	침해·피해 발생 우려 시(과태료 규정 외)	§64
개선권고	위반 아님	개인정보 보호실태 개선 필요 시	§61
징계권고	법 위반	개인정보 관계 법규 위반에 책임이 있는 자	§65
공 표	법 위반	위반이 심하여 공공에 경종 필요 시	§66

개인정보 실태조사

행정처분결과 공표제도(50개 기관)

행정처분 결과 공표제도*는 개인정보보호법 위반에 대한 행정처분 결과를 공개해 경각심을 고취하고, 유사사례 발생을 막기 위해 지난 2011년 도입된 제도

(근거)「개인정보보호법」제66조, 같은 법 시행령 제61조에 따라 내부지침으로 세부 공표기준 마련·시행

(목적) 당사자·관계자 경각심을 고취하여 경고적·예방적 효과를 달성하고 유사사례 발생 방지, 개인정보보호 법 질서 확립

기존 공표 제도 문제점 개선

주민등록번호를 포함한 고유식별정보 및 민감정보의 유출 등 중요 위반사항에 대하여 개인프라이버시 침해가능성이 매우 높은 경우임에도 불구하고 공표 대상에 포함되지 않는 불합리한 상황 발생

개인정보 실태조사

행정처분결과 공표제도(50개 기관)

구분	합계	2015년	2016년	2017년	2018년	2019년
합계	53	1	12	11	27	2
공공*	14	-	1	1	11	1
민간	39	1	11	10	16	1

- 2018(27곳)
  : 한국감정원, 베어트리파크, ㈜블루아일랜드개발, ㈜두산베어스, 더리본 주식회사, 성결대학교, 상지대학교, 명지대학교, 가톨릭대학교, ㈜금성출판사, 주식회사 좋은책신사고, ㈜골프존, 한국타이어(주), ㈜네이처리퍼블릭, 남양유업, ㈜탐앤탐스, 한국관광공사, 광주대학교, 에이치피코리아, ㈜하나투어, 부산도시공사, 경기도시공사, ㈜케이알티, 좋은라이프주식회사, 주식회사 케이디스포츠, 전쟁기념사업회

- 2017(11곳) : (주)대한항공, 이스타항공 주식회사, 롯데쇼핑㈜, 에이치케이저축은행, 인천항만공사, 비상교육, 정상제이엘에스, (주)파고다아카데미, (주)와이비엠에듀, 메가스터디교육, 일성레저산업(주)

- 2016(12곳) : 혜원의료재단, 인천국제공항공사, 남여주레저개발주식회사, 구로성심병원, 대한병원, 평택성모병원, 동인천길병원, 파인리조트, 더베이직하우스, 한국교원단체총연합회, 해태제과식품㈜, 애경유지공업㈜

- 2015(1곳) : 미래의료재단

개인정보 실태조사

기존 공표 제도 문제점

주민등록번호를 포함한 고유식별정보 및 민감정보의 유출 등 중요 위반사항에 대하여 개인프라이버시 침해가능성이 매우 높은 경우임에도 불구하고 공표대상에 포함되지 않는 불합리한 상황 발생

개선 공표 제도 주요 내용

아래 중 1개라도 해당되는 경우 공표

① 법위반 행위 은폐·조작 ② 주민등록번호 등 고유식별정보 및 민감정보의 분실·도난·유출·위조·변조·훼손으로 행정처분을 받은 경우 ③검사거부·방해

④ 법 제75조 제1항(5천만원 이하 과태료)에 해당하는 법 위반한 경우

⑤ 법 제75조 제2항(3천만원 이하 과태료) 2개 이상 위반한 경우

⑥ 법위반 상태 6개월 이상 지속 ⑦ 3년 이내 과징금·과태료·시정조치 2회 이상

⑧ 10만건 이상 유출사고 발생 ⑨ 2차 피해발생, 불법 매매

개인정보 실태조사

개선 공표 제도 변경 전후

분류	기존('14.8.5.~)	개정('19. 7. 10.~)	사유
위반내용	①다른 위반행위 은폐·조작	①다른 위반행위 은폐·조작	o현행 유지
		②주민등록번호 등 고유식별정보 및 민감정보의 분실·도난·유출·위조·변조·훼손으로 행정처분을 받은 경우	o<추가>유출에 따른 피해정도가 큼
		③검사거부·방해	o<추가>분류를 시정조치에서 위반내용으로 변경
위반정도	②1회 과태료 총액 1천만 원 이상, 과징금 부과	④법 제75조 제1항(5천만원 이하 과태료)에 해당하는 법 위반한 경우 ⑤법 제75조 제2항(3천만원 이하 과태료) 2개 이상 위반한 경우	o<변경>과태료 금액을 기준으로 한 공표 대신 중요 법위반 조항으로 변경(중앙부처 및 지자체 공표 가능) o<삭제>과징금 부과는 요건②해당하여 삭제
위반기간	③위반상태 6개월 이상 지속	⑥위반상태 6개월 이상 지속	o현행 유지
위반횟수	④3년 내 과징금, 과태료, 시정조치 2회 이상	⑦3년 내 과징금, 과태료, 시정조치 중 2회 이상	o현행 유지
피해범위	⑤유출·침해 피해자 수 10만 명 이상	⑧유출·침해 피해자 수 10만 명 이상	o현행 유지
피해결과	⑥2차 피해 발생, 불법 매매, 민감정보 침해	⑨2차 피해 발생, 불법 매매	o현행 유지
		⑩기타 사회적 비난이 높은 물의를 일으켜 행정처분을 받은 경우	o<추가>사회적 파장을 고려하여 공표기준에 반영
시정조치	⑦검사거부·방해, 시정조치 미이행으로 과태료 부과	<삭제>	o<삭제>검사거부·방해는 위반내용으로 분류하여 요건③으로 이동 o<삭제>시정조치미이행요건④에포함되어삭제

개보법 시행이후(2011년~) 위반 원인 분석

개인정보 유출사고와 개인정보 실태조사시(또는 조직의 개인정보 관리) 법위반사항이 발생되는 원인에 대해 분석하면 기관 내부의 문제, 법제도의 어려움, 해킹 등의 문제 등으로 구분됨

[개인정보보호법 시행 애로사항]

애로사항(복수응답)	비 율(%)
처리절차 복잡	40.6
법률의 이해	26.4
전문성 부족	21.0
인력 부족	20.3
예산 부족	19.5
문의처 찾지 못함	15.1
정부지원 부족	12.2
기 타	4.2

자료: 개인정보보호위원회·행정안전부(2018), 『2017 개인정보보호 실태조사』

1. (기관측면) 개인정보 조직(전문가) 부재, 예산부족, 내부관리
2. (정부측면) 법률 간 해석의 어려움(개보법, 망법, 신보법 등)
3. (법적측면) 개인정보 처리절차의 복잡성(수집-이용-제공-파기)
4. (해킹측면) 개인정보가 가지고 있는 금전적 가치
5. (신규기술적용) 클라우드, 빅데이터, IoT 등 적용 문제
6. (개인정보 준수 시점) 지속적 관리의 필요성(수집, 제공, 파기 등)

개보법 시행이후(2011년~) 위반 원인 분석

우리조직의 위치를 살펴보면 …

대부분 공공기관

	level 1	level 2	level 3
	개인정보보호법 상의 법의무사항이 수행되지 않거나 이에 대한 계획이 없는 조직	부분적으로 통제되거나 전체 통제 이후 이행관리가 부분적으로 않되는 조직.	법의무 사항을 준수하고 지속적으로 모니터링하며 개선을 수행하는 조직
조직	개인정보보호 조직 부재	개인정보보호 조직을 구성하거나 겸직	개인정보보호 조직을 별도로 구성
예산	개인정보보호 관련 예산 부재	개인정보보호 예산 수립 (충분한, 또는 충분지 못한)	개인정보보호 관련 충분한 예산 수립
인식	실태조사만 피하자 (유출은 글쎄?)	개인정보보호가 중요한데 매번 해야되? 교육을 또 받아? 양식만 있으면 되지....	최소한의 개인정보 수집, 개인정보보호를 위한 업무절차 개선 조직 구성원간의 책임과 역할이 명확
위반사례	동의양식 부재, 방침 부재 등 법상의 모든 위반사례 발생	조직 양식중 일부 미흡, 방침 현행화, 로그모니터링 미흡 지속적 관리사항, 신기술 등 관리미흡	내부인 개인정보 유출 위탁자 개인정보 관리미흡

II. 법조항별 위반사례

개인정보 처리단계별 보호조치

1.수집 / 2.이용

- 수집·이용 (15조)
- 최소 수집 (16조)
- 14세미만법정대리인동의 (22조)
- - 처리제한 -
  민감정보 (23조)
  고유식별정보 (24조)
  주민번호 (24조의 2)

3.제공

- 제3자 제공 (17조)
- 목적외이용·제공제한 (18조)
- 처리위탁 (26조)
- 국외이전 (17조)
- 영업양도·양수 (27조) (민간)

4.관리 (보관)

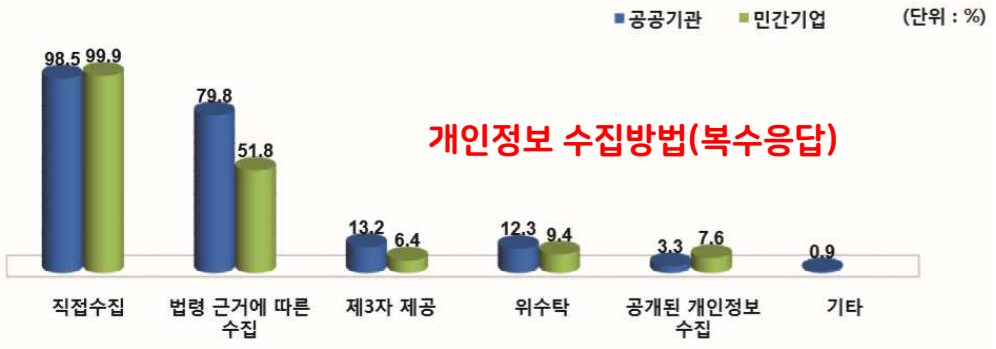
- 안전조치 의무 (29조)
- 처리방침 (30조)
  보호책임자 (31조)
- 개인정보유출 통지·신고(34조)
- 개인정보파일 등록 (32조) (공공기관)

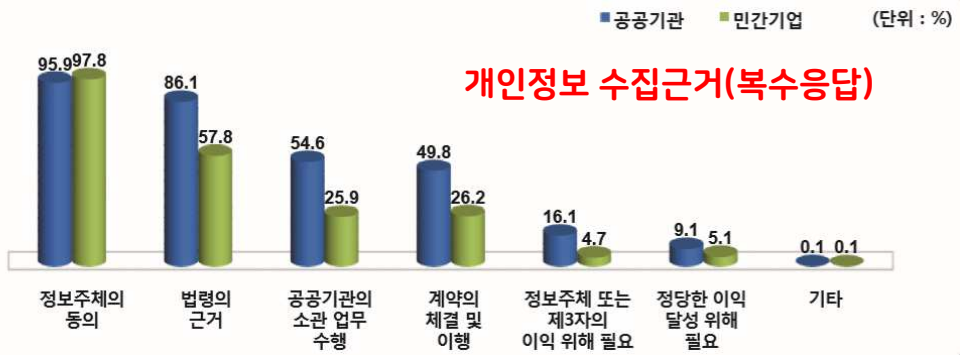
5.파기

- 파기 (21조)

개인정보보호법 제15조(수집.이용)

2018 실태조사





접수 유형	2012년	2013년	2014년	2015년	2016년	2017년	2018년
개인정보 수집 요건	3,507	2,634	3,923	2,442	2,568	1,876	2,764

2018년 개인정보침해 신고·상담 현황(KISA)

침해사례

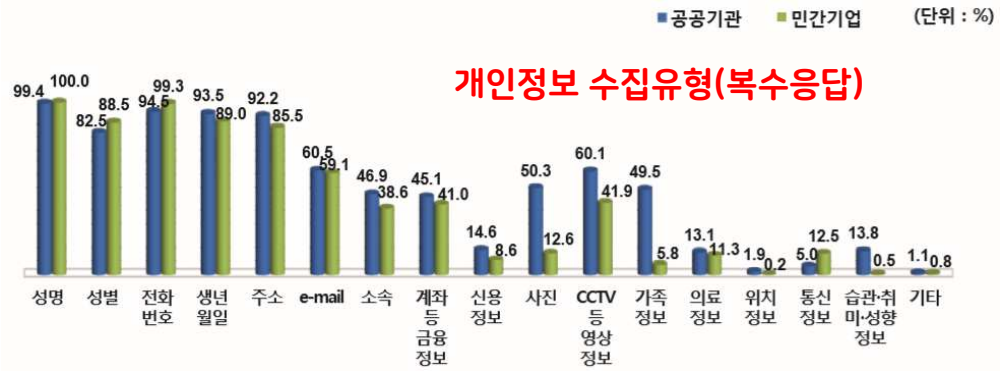
- 초등학교 앞에서 지나가는 초등학생을 대상으로 사탕을 주며 학생들의 이름, 학년, 부모의 휴대전화 번호를 동의 없이 수집 불가
- 명시적인 수신거부의사에 반하여 선거운동 목적의 정보를 전송하는 경우 1년이하의 징역 또는 100만원 이하 벌금
- A업체는 경양식점 프렌차이즈 업체로 바리스타 지원자 신청서에 개인정보 수집·이용시 정보주체 동의 미획득(실태조사, 5천만원 이하 과태료)
- 프렌차이즈 외식 업체 C사는 14세 미만의 정보주체의 개인정보를 수집할 때 법정대리인의 동의란이 없음(실태조사, 5천만원이하 과태료)
- 웹사이트에 공개한 휴대전화번호를 수집하여 광고문자를 발송한 것에 대한 손해배상 등 요구(분쟁조정, 손해배상)
- 병원 진료실에서 동의 없이 CCTV 촬영한 것에 대한 손해배상 등 요구(분쟁조정, 손해배상)
- 신청인의 동의 없이 명함을 습득하여 광고문자를 발송한 행위에 대한 손해배상 등 요구(분쟁조정, 손해배상)

대책 : 개인정보 파일현황 조사(부서, 방침, 행안부) → 수집근거 확인(법령, 동의) → 홍보 등 개별 동의 확인

5천만원이하 과태료

개인정보보호법 제16조(최소수집)

2018 실태조사



접수 유형	2012년	2013년	2014년	2015년	2016년	2017년	2018년
과도한 개인정보 수집	847	1,139	1,200	868	390	681	553

2018년 개인정보침해 신고·상담 현황(KISA)

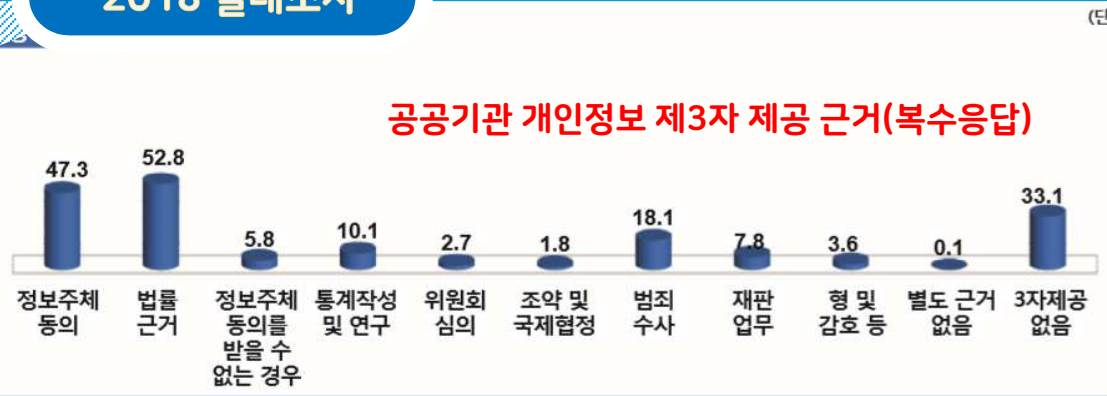
대책 : 개인정보 파일별 수집항목 조사 → 동의(개인정보 항목의 필요성 검토, 업무담당자 및 유사업무 고려) → 개인정보 수집이용동의서 개정

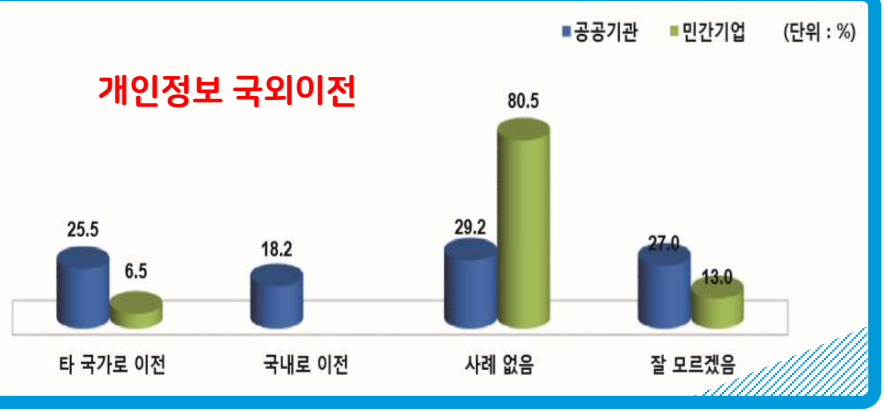
3천만원이하 과태료

(법령평가위원회 개인정보 침해요인 평가) 한자이름, 법인대표자 주소, 주민등록등본(초본 대체), 우편물 외부에 독촉장 기재 등)

개인정보보호법 제17조(제3자 제공)

2018 실태조사





사례

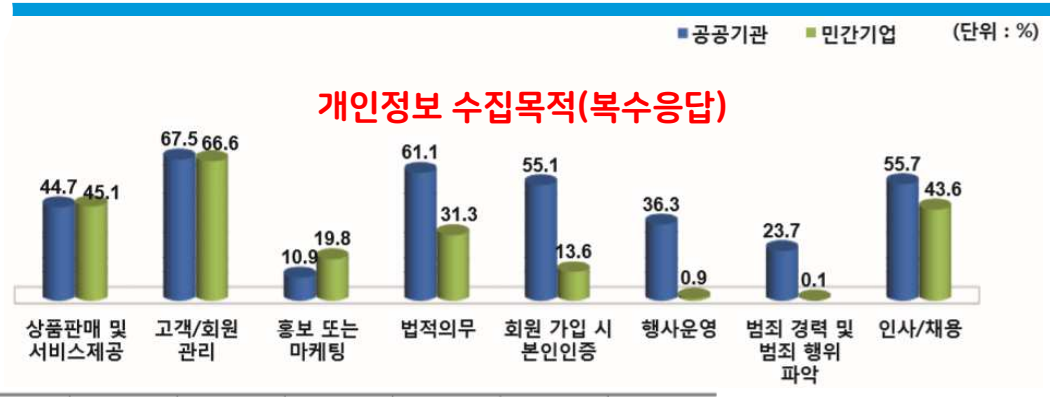
- 외교부의 재외국민 등록자 개인정보 제공에 관한 건(2017.9.25.) : 외교부 수집(재외국민등록법) vs 서울특별시, 국세청, 한국자산관리공사가 지방세 징수, 국세 징수, 공 매 대행업무를 각 수행 목적 으로 개인정보 제공 가능(위원회의결)
- 온라인 쇼핑 사이트인 A사는 개인정보 제3자 제공에 대한 정보주체 동의 미획득(5년 이하의 징역 또는 5,000만 원 이하의 벌금, 실태조사)
- 의료기관인 B사 개인정보 제3자 제공 동의 시 필수 고지 사항 누락(3천만원이하의 과태료, 실태조사)
- 학교법인의 진상조사 기록을 동의 없이 교원소청심사위원회에 제출한 것에 대한 손해배상 등 요구(분쟁조정, 손해배상)
- 보험 정보를 동의 없이 조회하고 가족에게 제공한 것에 대한 손해배상 등 요구(분쟁조정, 손해배상)

대책 : 부서별 제공현황 파악(부서, 방침, 제공대장) → 제공근거 확인(법령, 동의)
→ 제공시 동의(법령), 범위 확인

5년 이하의 징역 또는
5천만원 이하의 벌금

개인정보보호법 제18조(목적외이용)

2018 실태조사



접수 유형	2012년	2013년	2014년	2015년	2016년	2017년	2018년
목적 외 이용 또는 제3자 제공	2,196	1,988	2,242	3,585	3,141	3,881	6,457

2018년 개인정보침해 신고·상담 현황(KISA)

침해사례

- 개인정보의 상업적 판매(대법원 2017.4.7. 선고 2016도13263 판결) : 경품행사 모집된 정보 7개 보험사 판매(1,694만건, 231억)
- 교육사이트에서 회원 탈퇴를 했음에도 동의 없이 홍보 이메일을 발송한 행위에 대한 손해배상 등 요구(분쟁조정, 손해배상)
- 성형수술 전후 사진을 동의 없이 병원 홍보에 이용한 것에 대한 손해배상 등 요구(분쟁조정, 손해배상)

대책 : 개인정보 이용 현황(Log 분석) → 목적 외 이용내역 확인(교육, 징계 등)

5년 이하의 징역 또는
5천만원 이하의 벌금

개인정보보호법 제21조(파기)

2018 실태조사

접수 유형	2012년	2013년	2014년	2015년	2016년	2017년	2018년
개인정보 미파기	779	602	686	767	545	723	1,036

2018년 개인정보침해 신고·상담 현황(KISA)

침해사례

- A업체는 가전제품 소매업과 이동 전화 판매·개통 서비스를 제공하는 업체로 B씨가 몇가지 정보만 이야기하니 한참 만에 방문한 것 같다고 B씨의 개인정보를 말하는 것, 상법(5년)지난 정보 미파기(실태조사, 3,000만 원 이하 과태료)
- A씨는 지역 민원과 지방자치단체 관청인 B기관의 홈페이지에 민원 요청 글을 남긴 이력이 있고 이후 탈퇴 실태조사결과, 2005년 부터 탈퇴한 회원(약 2,800명)의 개인정보가 파기되지 않은 채 보관(실태조사, 3천만 원 이하 과태료)
- A사는 여행 알선 업체로, 온라인 10%, 오프라인 90%의 비율로 매출발생, 2010년과 2011년에 수집된 예약 고객 정보 1018여 건의 경우 5년 이상 지난 개인정보 미파기(실태조사, 3천만 원 이하 과태료)
- 휴면 처리된 계정의 개인정보를 이용한 행위에 대한 손해배상 요구(분쟁조정, 손해배상)

대책 : 개인정보 파일(보유기간) 확인 → 온, 오프라인 파기 현황 파악 → 분리보관 현황 파악

5년 이하의 징역 또는
5천만원 이하의 벌금

개인정보보호법 제22조(동의방법)

2018 실태조사

접수 유형	2012년	2013년	2014년	2015년	2016년	2017년	2018년
개인정보 수집시 고지·명시 의무	396	84	268	65	54	69	112

2018년 개인정보침해 신고·상담 현황(KISA)

분쟁조정

- 개인정보 상업적 판매(대법원 2017.4.7. 선고 2016도13263 판결) : 경품행사 모집된 정보 7개 보험사 판매(1,694만건, 231억), 1mm고지
- C회사는 자체 홈페이지를 운용, 개인정보 수집·이용시 필수 고지 사항 누락(동의거부와 ….) : 3천만원이하 과태료(실태조사)
- A업체 사이트를 방문한 B 씨는 여러 호텔을 비교해 가격비교 실시, 비회원예약시 개인정보 수집, 이용동의와 홍보 동의를 일괄로 받음 (실태조사, 1천만원 이하의 과태료)
- A씨는 B업체 쇼핑몰에서 쇼핑을 하다가 신규 회원으로 가입하면 바로 사용이 가능한 적립금을 추가로 준다는 공 지를 보고 회원 가입하였으나 개인정보 수집·이용동의 내용에 '새로운 서비스나 신상품, 이벤트 정보 등 최신 정보 안내'가 수집 목적에 포함되어 있음(실태조사, 1천만원 이하의 과태료)

개인정보보호법 제23조(민감정보)

민감정보

사상, 신념, 노동조합·정당가입,
건강정보, 유전정보, 범죄경력 정보

침해사례

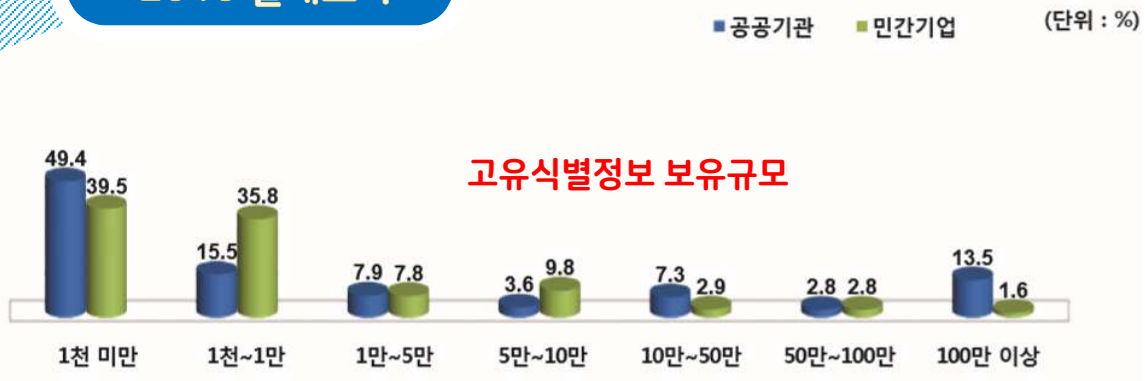
- 광주광역시 공무원노동조합 조합비 소득공제 내역의 감사목적 제공에 관한 건 (2017.6.26.) : 노동조합비(민감정보) vs 공공감사에 관한법률
- (법령의 민감정보의 처리 요구 허용하는 경우, 「공무원의 노동조합 설립 및 운영 등에 관한 법률에 따른 노동조합 가입·탈퇴 등 감사)(위원회)

대책 : 민감정보 수집이용 현황 확인 → 수집근거(법령, 별도동의), 목적(입증책임)

5년 이하의 징역 또는
5천만원 이하의 벌금

개인정보보호법 제24조(고유식별정보)

2018 실태조사



고유식별정보

주민등록번호, 여권번호,
운전면허번호, 외국인등록번호

침해사례

- 고유식별정보 별도 동의사항을 위반한 사례
- 고유식별정보에 대한 안전성 확보조치 미흡사례
- 개인정보 영향평가 수행 미흡

대책 : 고유식별정보 수집이용 현황 확인 → 수집근거(법령, 별도동의) → 대체수단 도입 여부 검토

5년 이하의 징역 또는
5천만원 이하의 벌금

개인정보보호법 제24조의2(주민번호처리제한)

다음의 어느 하나에 해당하는 경우에만 주민등록번호 처리 가능

- 법률·대통령령·국회규칙· 대법원규칙 · 헌법재판소규칙· 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
- 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 보호
- 위의 사항에 준하는 경우로서 행정안전부령으로 정하는 경우

인터넷으로 회원 가입 시 본인확인이 필요한 경우, 주민번호 대체수단을 제공하여야 함

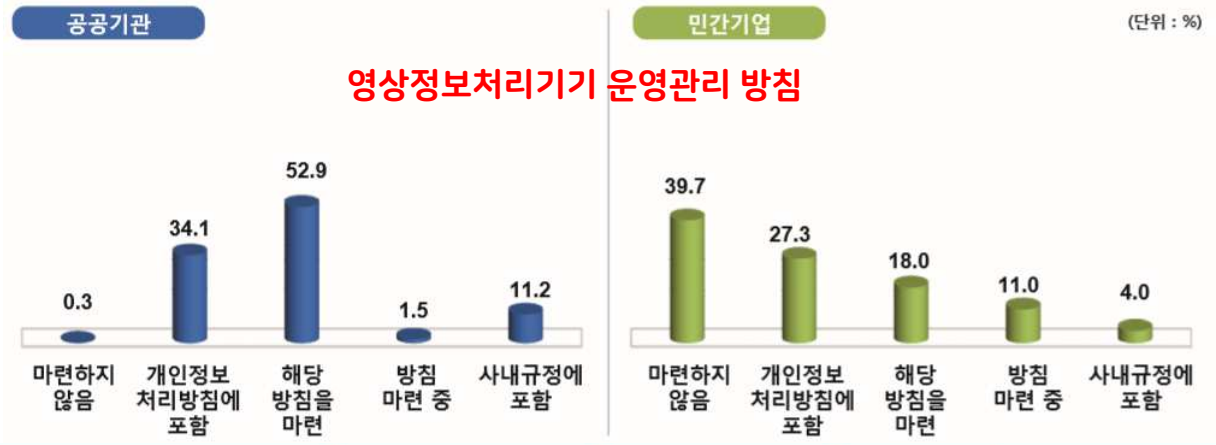
- (예) I - PIN, 휴대폰, 공인인증서, 전자서명 등

침해사례

- A협회에서는 국가 자격 검정 및 교육 관련 업무 등을 온라인상에서 지원하고 처리하는 홈페이지 운영, 법적 근거 없는 주민등록번호 수집 (실태조사, 3천만 원 이하 과태료)

개인정보보호법 제25조(영상정보처리기기)

2018 실태조사



기관명	파일 수(개)	영상정보처리기기(대)	기관명	파일 수(개)	영상정보처리기기(대)
감사원	7	82	보건복지부	146	1,324
국가정보원	-	-	환경부	81	523
산업통상자원부	21	370	합 계	112,653	331,537

위반사례

- 영유아보육법 어린이집 CCTV 설치 및 운영에 관한 헌법소원(헌재, 2017.12.28.선고 2015헌마994 결정) : 공익 vs 사익
- 지방자치단체 통합관제센터 영상정보의 군부대 제공에 관한 건(2017.10.16.) : 훈련시 영상제공 및 CCTV 조작 가능(위원회)
- 주차장에서 촬영된 CCTV 열람 요청 거부에 대한 손해배상 등 요구(분쟁조정, 손해배상)

대책 : cctv 현황 파악 → 방침, 녹음, 목적 등 확인 → cctv 안전성 확보기준 준수 확인

목적 위반, 녹음 : 3년 이하의 징역 또는 3천만원 이하의 벌금
운영 위반 : 3천만원 이하 과태료
안내판 : 1천만원 이하 과태료

개인정보보호법 제26조(업무위탁)

2018 실태조사

접수 유형	2012년	2013년	2014년	2015년	2016년	2017년	2018년
개인정보 처리 위탁	125	44	40	22	25	73	141

2018년 개인정보침해 신고·상담 현황(KISA)

침해사례

- A병원은 연매출 100여 억 원, 상시 종업원 160여 명 규모의 종합 병원으로 홈페이지와 EMR(Electronic Medical Record, 전자 의무 기록) 시스템을 위탁관리하나 위·수탁계약서상 법정 필수 기재 사항 누락(실태조사, 1천만 원 이하 과태료)
- A항공사는 국내 B항공사의 자회사로 국내 항공사 매출 기준으로 비교적 안정적인 순위를 유지, 전산·유지보수 업무에 대해서는 C업체에 위탁하여 관리(실태조사, 1천만 원 이하 과태료)
- 국내 임대 및 건설 관련 업무를 하고 있는 B업체는 대표 홈페이지, 시설 관리 시스템, 분양 임대 관리 시스템의 유 지 보수를 위하여 C, D, E 업체와 각각 개인정보처리 업무 위·수탁계약을 맺고 있으나 미고지(실태조사, 1천만 원 이하 과태료)
- C리조트는 홈페이지를 위탁한 업체 D업체에 대한 개인정보 교육 등 개인정보처리 업무 수탁자 관리 감독 미흡

대책 : 부서별 위탁 현황 파악(방침, 계약서 등) → 관리감독 모니터링(교육, 기술적 조치)
→ 계약 종료 후 파기여부 확인

1천만원이하 과태료

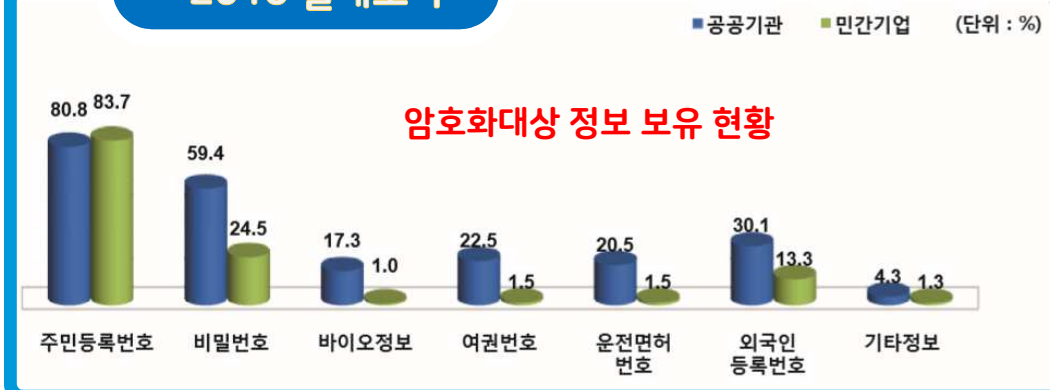
개인정보보호법 제27조(영업양도)

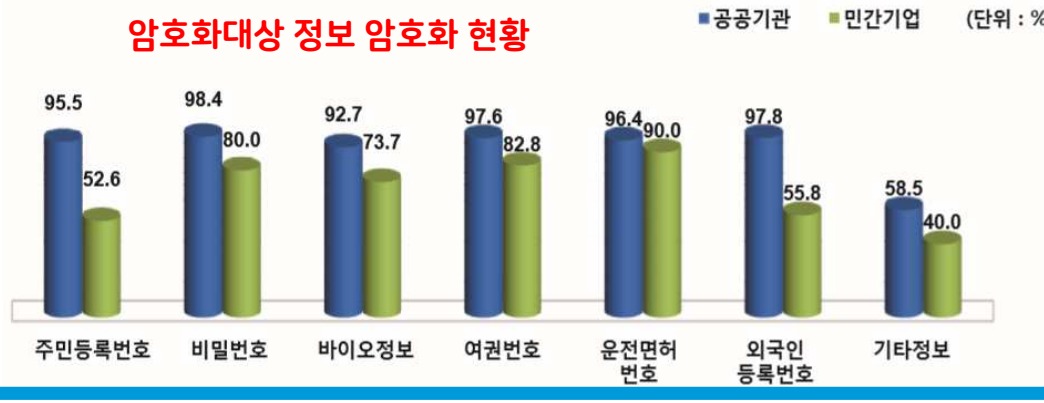
위반사례

- 재작년에 A병원에서 수술을 받은 D씨는 얼마 전 A병원이 없어진 것을 알게됨. 그리고 이웃으로부터 A병원 이 근처 B병원과 합병하여 C병원으로 더 크게 재설립되었다는 소식을 들음. C병원에서 문의해보니 자신의 개인정보가 이전된 사실을 알게됨
  (실태조사, 1천만 원 이하 과태료)

개인정보보호법 제29조(안전조치의무)

2018 실태조사





침해사례

- 직원의 부주의에 의한 전자팩스 전송을 통한 개인정보 유출 사건(2018.3월, 387명)
- 초등학교 가정통신문 발송시 기초생활 수급자의 개인정보를 노출하여 발송
- 고객의 물품을 배송하는 C업체는 목적이 달성된 개인정보(배송이 완료된)를 배송이 완료되지 않은 개인정보와 분리보관 미수행 (실태조사, 1천만 원 이하 과태료)
- B대학 병원은 직원들의 개인정보가 ERP(Enterprise Resource Planning) 시스 템에 저장·관리되고 있으나 암호화 미적용(실태조사, 3천만 원 이하 과태료)
- C항공사 홈페이지에서 여권번호를 기입하도록 되어 있으나 평문으로 저장(실태조사, 3천만 원 이하 과태료)
- A병원은 30만 건 이상의 환자 개인정보를 보관, 개인정보처리시스템을 도입하여 운용하나 내부 관리계획 미수립(실태조사, 3천만 원 이하 과태료)
- B업체는 호텔·콘도·스키장·골프장등 종합 레저 사업을 하는 업체 개인정보처리시스템 도입 운영하고 있으나 비밀번호 작성 규칙 미수립(실태조사, 3천만 원 이하 과태료)
- B업체는 여행 중계 업체 비밀번호 평문저장 등 관리 소홀(실태조사, 3천만 원 이하 과태료)
- 민간 건설업체인 A사는 개인정보처리시스템의 비밀번호 횟수 제한 정책 미적용(실태조사, 3천만 원 이하 과태료)
- A업체는 학습지·학습서적 출판업체는 홈페이지 계정 비밀번호 전송 구간 암호화 미흡 (실태조사, 3천만 원 이하 과태료)
- 공공 업무를 수행하는 A기관은 개인정보처리시스템 접속기록 항목 누락 (실태조사, 3천만 원 이하 과태료)

개인정보의 안전성 확보조치 기준 개정(6.7)

고시 변경 배경

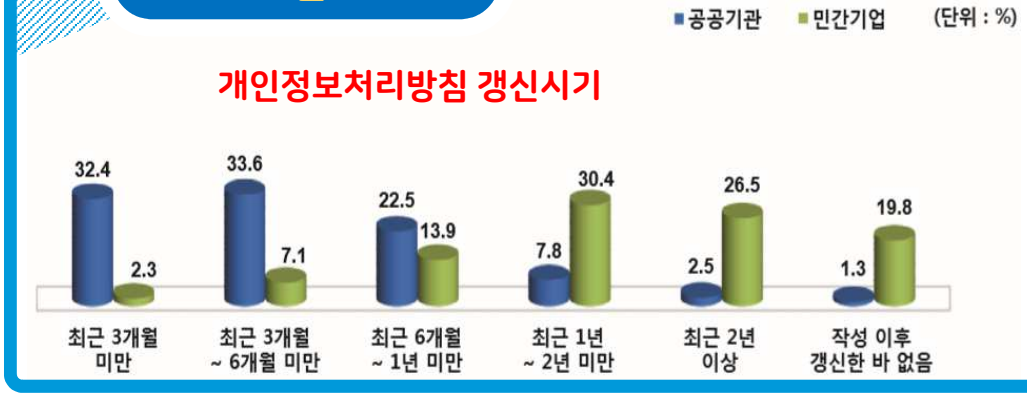
- 접속기록 6개월 보관이 되레 관리부실 초래(18.8.21, 한겨레신문)
  ※ 2012년 총선 당시 서울 서대문구 13만명의 개인정보 불법 활용 정황
- 접속기록 관리부실로 무단열람 발생('12~'16 간 1만7천명 소명, 2,213건 징계('17 복지부 국감자료))
- 개인정보 유출사고 발생 1~2년 후 추적(한국은 사이버침해사고 발생 이후 발견시간은 2년 9개월, 2018, FireEye)
- 정보통신망법(기간통신사업자 2년), 신용정보보호법(감독규정 1년이상)

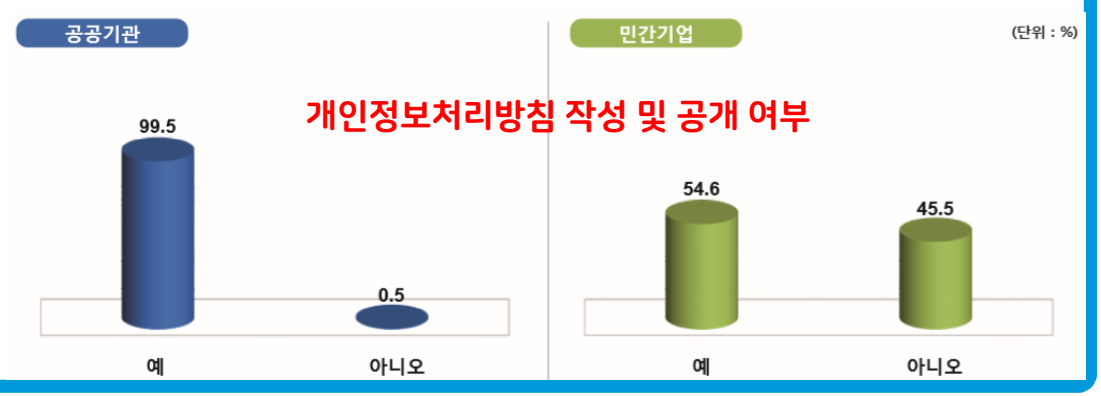
주요 내용

- 제2조(정의) 접속기록의 범위 확대 : 계정, 접속일시, **접속지 정보**, 접속자 정보, 수행업무
  ※ 접속한 자의 PC, 모바일기기 등 단말기 정보 또는 서버의 IP주소 등 접속 주소
- 제4조(내부관리계획의 수립 시행)
  ※ 개인정보 보호책임자는 <u>접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상으로</u> 점검·관리 하여야 한다.
- 제8조 (접속기록의 보관 및 점검) 접속기록은 1년이상 보관, 월 1회 이상 점검
- 5만명 이상 고유식별정보 또는 민감정보를 처리하는 경우 2년 이상 보관

개인정보보호법 제30조(처리방침)

2018 실태조사





침해사례

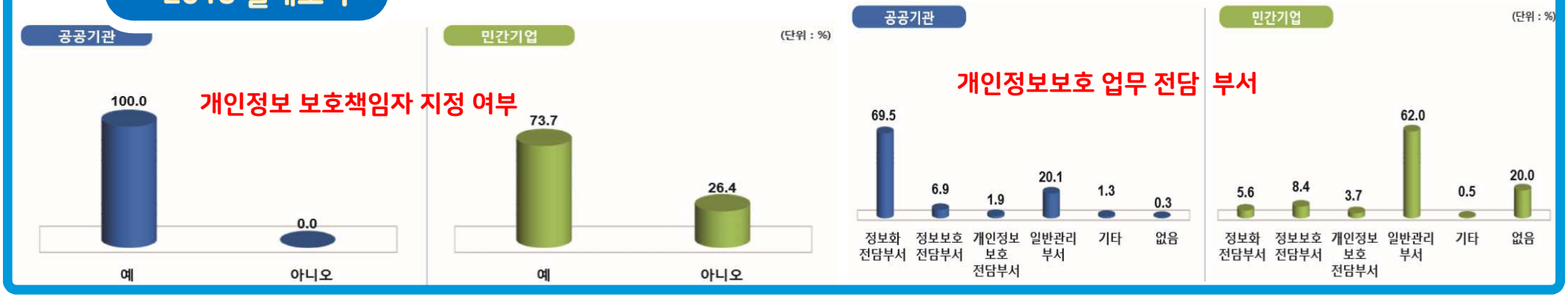
- A기관은 택지 개발 및 공동 주택 분양, 시설물 관리, 임대 등의 업무를 수행하는 기관으로 개인정보처리방침 내 처리 목적, 보유기간, 항목 누락(실태조사, 1천만 원 이하 과태료)
- 35만건 개인정보를 관리하는 B병원은 개인정보처리방침 내 수집 목적, 제3자 제공, 위탁, 파기 누락(실태조사 1천만원과태료)

대책 : 개인정보처리방침 확인(웹사이트별) → 매년 파일, 위탁 등 변경사항 반영 확인

1천만원이하 과태료

개인정보보호법 제31조(책임자지정)

2018 실태조사



침해사례

- A사는 가구 및 인테리어 자재를 취급하는 업체로, 대표 홈페이지와 쇼핑몰을 운영하고 있으나 개인정보 보호책임자 미지정(실태조사, 1천만 원 이하 과태료)
- A대학교는 특별 전형, 수시, 정시 등의 입시 전형 기간에 분산하여 지원하고 있는 입시 지원자들을 효율적으로 관리하기 위하여 온라인 홈페이지를 운용하고 있으나 A대학교는 이러한 업무를 총괄하여 책임지는 개인정보 보호책임자로 전산 담당부서장인 정보 처장을 지정(실태조사, 1천만 원 이하 과태료)

개인정보보호법 제32조(파일등록 및 공개)

2018백서

구분	기관명	파일 수	개인정보 건수
	제주특별자치도	2,020	200,760,161
	총계	298,275	122,519,027,505

침해사례

- A협회는 관련 특별법에 따른 특수 법인으로, 다양한 사업을 관리하고 운영하는 특성상 대량의 개인정보를 수집·처리하고 있음.
  A협회의 경우 개인정보 보호법상 공공기관에 해당하나 현장점검 결과, A협회가 공공기관임에도 불구하고 해당 개인정보 보호책임자는 개인정보파일의 명칭, 운 영 근거 및 목적, 기록되는 개인정보 항목, 처리 방법 및 보유기간 등의 개인정보파일 등록 사항을 담은 운용 현 황, 즉 개인정보파일을 행정안전부장관에게 등록하지 않음(실태조사)

행정안전부 KISA Korea Internet & Security Agency

Privacy by Trust, Trust by Privacy!

질의문답