

- Part 3 -

사업자의 공동된 오류



행정안전부



한국인터넷진흥원

목차

1. *Safe Office*개요와 주요 점검 결과
2. 관점별 개인정보 보호 현안
3. 공통된 오류 사례와 개선방안

본 내용은 2010년 행정안전부와 KISA가 추진한 'Safe Office – 개인정보 보호 체계구축 지원사업' 시 적용한 개인정보 보호 관련 33개 점검항목 결과를 바탕으로 도출한 자료입니다.



행정안전부



1

***Safe Office*개요와 주요 점검 결과**



행정안전부



한국인터넷진흥원

1. Safe Office 개요와 주요 점검 결과

Safe Office
-개인정보 보호
체계 구축
지원사업

중소규모 사업자
(비 IT 업종)

사업자 신청
및 선정

사전점검

결과보고서 및
개선방안 도출

인터뷰 및 상담

현장점검

사업자의 개인정보 보호
관리적·기술적 조치 현황 파악

동종업계 현황 파악

공통오류사항 및 개선방안 제시

1. Safe Office 개요와 주요 점검 결과

점검항목별 결과

<점검항목은 2010년 법령 기준임>

점 검 항 목			◎◎사	★★사	◇◇사	●●사	△△사	■ ■ 사	▣ ▣ 사	▼ ▼ 사	○○사	◆ ◆ 사
법적 준수 요건	수집/이용	개인정보 수집·이용 동의	●	○	○	○	●	○	●	●	●	○
		민감정보 수집	●	○	○	○	○	○	○	●	○	○
		고유식별정보 처리 제한	-	-	-	-	-	-	○	-	-	-
		목적 외 이용금지	○	○	○	○	○	○	●	●	○	○
	위탁·제공	제3자 제공	-	-	-	-	-	○	●	●	○	○
		취급/처리위탁	●	●	●	●	●	○	●	●	○	●
		개인정보의 이전	-	-	-	-	-	-	●	-	-	-
		동의 받는 방법	●	○	○	○	○	○	●	●	●	○
	관리 및 파기	개인정보 관리책임자 지정	●	○	○	●	●	○	○	○	○	○
		개인정보 처리방침 공개	●	○	○	○	○	○	○	○	○	○
		개인정보 보호조치	●	●	●	●	●	●	●	-	●	●
		개인정보 누설금지	●	●	●	●	●	●	●	●	○	○
		개인정보 파기	-	-	●	-	●	●	●	○	○	○
	이용자 권리	이용자의 권리	●	-	-	-	-	-	-	-	-	-
		법정대리인 권리	●	-	-	-	-	-	-	-	-	-
		손해배상	●	-	-	-	-	-	-	-	-	-

< 범례 > ● : 미흡, ● : 부분미흡, ○ : 만족, '-' : 해당사항 없음 또는 판단불가

1. Safe Office 개요와 주요 점검 결과

점검항목별 결과

<점검항목은 2010년 법령 기준임>

점 검 항 목			◎◎사	★★사	◇◇사	●●사	△△사	■ ■ 사	▣ ▣ 사	▼ ▼ 사	○○사	◆ ◆ 사
기술적·관리적 보호조치	관리적 조치	내부관리계획 수립	●	●	●	●	●	○	●	●	●	○
		내부지침 마련	●	●	●	●	●	○	●	○	○	○
		물리적 접근방지조치	-	●	●	●	○	●	●	○	○	○
		정기 자체 감사	●	●	●	●	●	●	●	●	●	○
	기술적 보호조치	식별 및 인증 조치	○	●	●	○	○	○	○	●	○	○
		방화벽설치 등 조치	○	●	○	○	○	○	○	○	○	○
		전송암호화 등 조치	○	●	●	●	○	●	○	●	○	○
		저장암호화 등 조치	○	●	●	●	-	●	○	●	●	○
		위·변조 방지 조치	●	●	●	●	●	●	●	●	●	○
		보안프로그램 설치운영	○	○	○	○	○	○	○	○	○	○
개인정보 처리방침	개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법		●	○	○	○	●	○	●	●	●	○
	제3자에게 제공하는 경우 제공 받는 자의 성명, 제공 받는 자의 이용 목적과 제공하는 개인정보의 항목		●	○	○	○	○	○	●	●	○	○
	개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법		●	●	○	○	●	○	●	○	○	○
	개인정보 취급위탁을 하는 업무의 내용 및 수탁자		●	●	●	○	●	○	●	●	○	○
	이용자 및 법정대리인의 권리와 그 행사방법		●	○	○	○	○	○	○	○	○	○
	인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치운영 및 그 거부에 관한 사항		●	○	○	○	○	○	○	○	○	○
	개인정보 관리책임자 성명 또는 관련부서 명칭과 그 전화번호 등 연락처		●	○	○	○	○	○	○	○	○	○

< 범례 > ● : 미흡, ● : 부분미흡, ○ : 만족, '-' : 해당사항 없음 또는 판단불가

2

관점별 개인정보 보호 현안



행정안전부

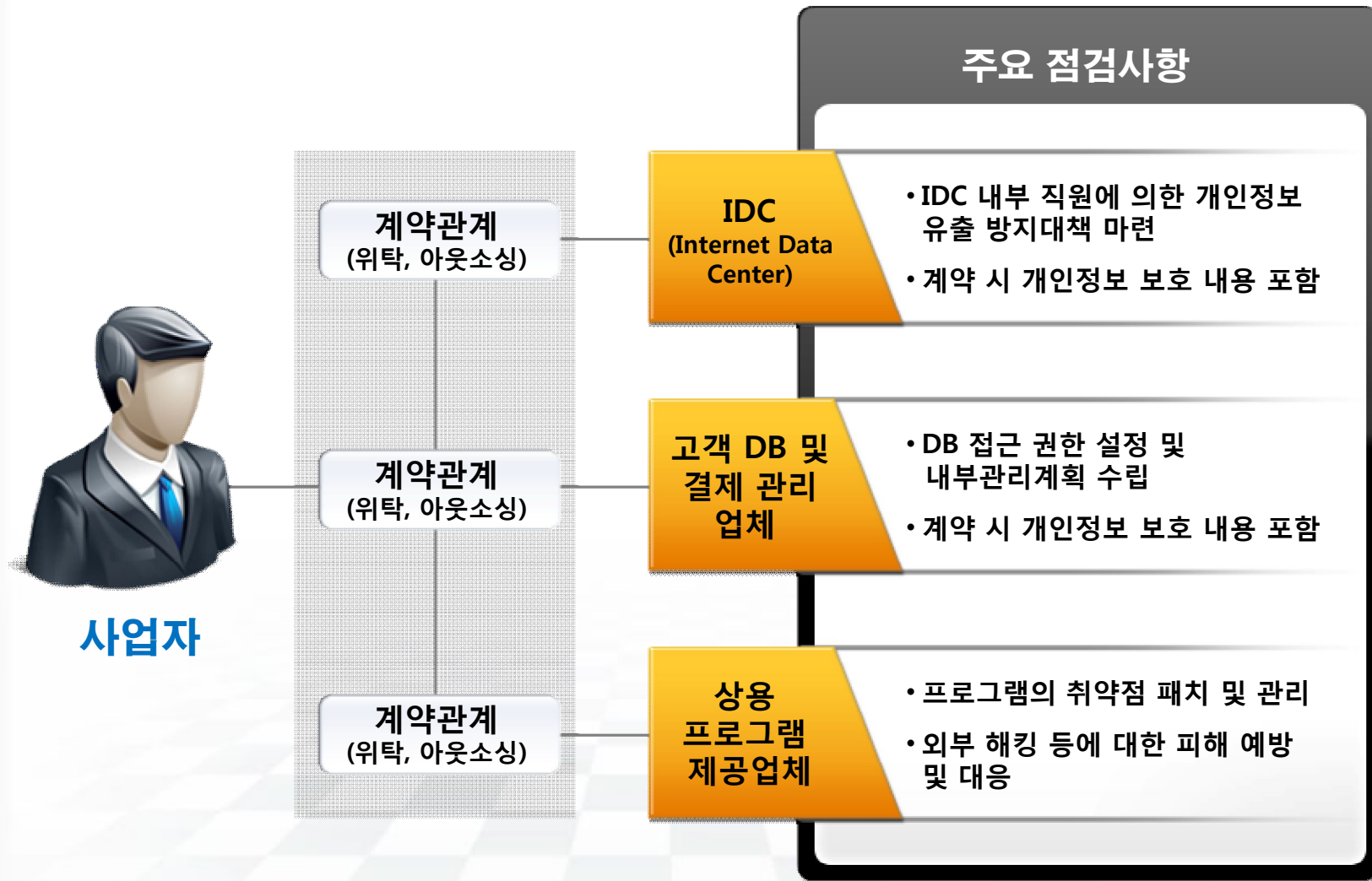


한국인터넷진흥원

2. 관점별 개인정보 보호 현안



2. 관점별 개인정보 보호 현안



3

공통된 오류 사례와 개선방안



행정안전부



한국인터넷진흥원

3. 공통된 오류 사례와 개선방안

종이를 통한 수집에도 고지와 동의는 필수!

**오프라인 정보 수집 시
동의 및 고지 절차 생략**

2011년 고객사은대잔치

고객님의 사랑에 감사드리며,** 나라가 작은선물을 마련했습니다.
(**나라가 전국55개 대리점 방문고객님 모두에게 온 수저를 드립니다.)

**행사기간 중 대리점에 방문하는
고객님께 추첨을 통해
경품을 드립니다.**

(행사기간 : 2011년 3월 1일~2011년 6월 30일)
(당첨자 발표 : 2011년 7월 14일)

<경품>
 1등 - LCD TV
 2등 - 스팀 청소기
 3등 - 문화상품권
 특별상 - 순채

**** 나라 경품응모권**

이 름 :

주 소 :

전화번호 :

주민번호앞자리 :

응모일,응모점 :



공통 오류내용

오프라인을 통한 개인정보 수집 시 동의 및 고지절차 생략

- 종이 형태의 교육신청서
- 이벤트 응모권
- (여행사 등의) 방명록 등에 동의 및 고지절차 생략



개선방안

개인정보 수집/이용 동의 약식 샘플(종이문서)

OOO회사는 _____ 특별 이벤트 진행을 위해 아래와 같이 개인정보를 수집/이용 하는 내용을 관계 법령에 따라 고지하오니, 동의해주시기 바랍니다.

<수집/이용 항목>

이름, 전화번호, 이메일 주소

<수집/이용 목적>

이벤트 응모 및 상품 제공, SMS발송 등

수집한 개인정보는 본 수집/이용 목적 외에 다른 목적으로 사용되지 않습니다.

<이용, 보유 기간>

이벤트 기간 내 단, 이벤트가 종료된 후 고객정보는 폐기 됩니다.

☐ 동의 ☐ 동의하지 않음

기타 개인정보 처리에 관한 상세한 사항은 OOO 회사의

홈페이지(<http://www.ooo.oo.kr>)에 공개한 "개인정보 처리방침"을 참조 하십시오.

3. 공통된 오류 사례와 개선방안

주민번호만이 유일한 수단은 아니다!

 주민번호 대체수단을 도입하지 않은 경우

실명확인

이름 (이름 사이의 공백에 없도록 꼭주십시오.)

주민등록번호 - (실명확인후 아이디를 가입할 수 있습니다.)

실명 확인 >



공통 오류내용

본인인증 시 주민등록번호만 이용

- 본인인증 : 실명, 주민번호 확인
- 회원가입 시 주민번호 입력



개선방안

- 실명 인증 시 주민번호 이외의 인증방안 제시
(ex : i-PIN, 공인인증서 등 적용)

실명인증

아이핀(i-PIN) 인증

이름

주민등록번호 -

실명인증

아이핀(i-PIN) 인증을 통한 가입을 원하시면
i-PIN인증 버튼을 눌러 회원가입을
진행해 주세요.

i-PIN인증

2009년 4월 1일 개정된 주민등록법 제37조(합칙) 제10호에 의해
타인의 정보 및 주민등록번호를 도용하여 사용하는 경우 3년 이
하의 징역 또는 1천만원 이하의 벌금에 처해지게 됩니다.

아이핀(i-PIN)은 웹사이트에 주민등록번호 대신 인증할 수 있는
사이버 신원확인번호로서 인터넷 상에서 주민등록번호가 무단
으로 유출되어 도용되는 부작용을 막기 위해 만들어진 서비스입
니다.

3. 공통된 오류 사례와 개선방안

회사 내 저장된 개인정보를 누군가 몰래 열람한다!

개인정보 접근자를 위한 보안 서약서

개인정보 보호 서약서

나 ()는 업무 중에 알게 된 개인정보 및 회사의 업무와 관련된 정보에 대하여 업무 수행중이나 업무 수행 후에도 비밀을 지킬 것을 서약합니다.

또한 회사에서 수집한 개인정보의 보호를 위해 회사에서 정하는 개인정보 보호 관리 규정을 준수할 것이며, 적정한 절차 없이 개인정보를 무단으로 조회, 누출하지 않을 것을 서약합니다.

개인정보 보호와 관련한 비밀의 준수와 개인정보 보호를 위한 법적 준수기준인 "개인정보 보호법"에 명시된 모든 조항과 회사의 개인정보 보호 관리 규정 등 관련된 모든 조항이 포함된다는 것을 충분히 설명 받고 숙지하였습니다.

만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유 없이 조회, 유출, 오용할 경우, 형사상 민사상의 법률 조항에 의거하여 제재를 받을 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

일 시: 201 년 월 일
소 속:
성 명: (인)



공통 오류내용

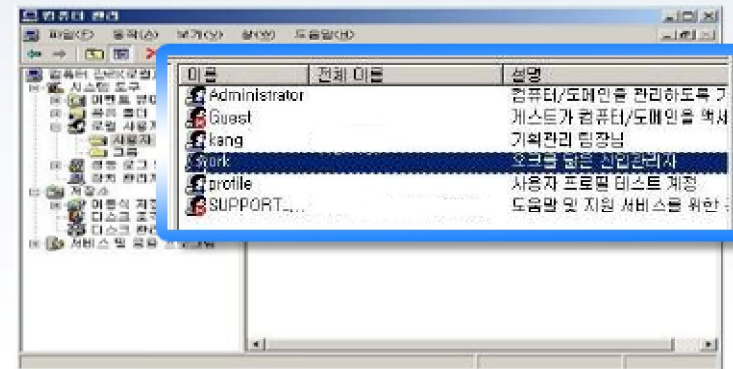
개인정보 접근 권한자 미분류

- 개인정보 파일 접근 계정을 하나의 아이디로만 운영
- 내부 직원에 대한 개인정보 유출, 오남용 방지 방안 부재
- 개인정보 파일 접근자 로그관리 및 감사



개선방안

- 접근 계정 직무별, 담당자별 구분 및 로그 관리
- 개인정보 접근자에 대한 보안 서약서 징구



- 직원 계정 관리 예제 -

3. 공통된 오류 사례와 개선방안

수탁업체도 내 회사처럼!

취급위탁 사업자를 위한 보안 서약서

개인정보 위탁(제공) 계약 보안 서약서

_____(이하 "을"이라 한다)는 OOOO회사(주) (이하 "갑"이라 한다)의 개인정보 취급위탁 업무수행에 따른 개인정보 및 개인정보취급 시스템(DBMS)의 안전한 보호를 위해 아래 각 호의 사항을 준수한다.

1. 을은 갑의 정보보호 규정을 준수하며 갑이 위탁한 개인정보(정보 및 정보시스템)를 안전하게 사용·관리하며, 개인정보의 보호를 위해 다음의 사항을 준수한다.
 - 1) 갑의 정보보호 규정 및 개인정보 보호 관련 법규의 준수
 - 2) 업무상 알게 된 개인정보에 관한 비밀 유지
 - 3) 제공받은 목적외 제공 금지
 - 4) 제공받거나 허가받은 개인정보 처리업무 및 권한의 제3자 공유 금지
 - 5) 취급업무의 종료 시의 파기 등 의무사항의 이행
 - 6) 갑의 규정 및 관련 법규의 미준수 또는 관리소홀로 인해 발생한 개인정보 사고에 대한 책임 부담
2. 을은 갑의 업무 수행을 위해 담당하는 직원에 대하여 책임을 진다.
3. 을은 갑의 사전 승인을 받지 못한 프로그램 및 정보기기는 갑의 업무와 관련하여 사용하지 않는다.
4. 을은 갑의 정보보호 정책과 반하는 행위로 야기되는 문제에 대해 민·형사상 책임을 진다.

상기사항을 숙지하고 이를 성실히 준수할 것을 서약함

일 시: 201 년 월 일
소 속:
성 명: (인)



공통 오류내용

개인정보 위탁 관리감독 방안 부재

- 취급위탁 사업자(수탁자)에 대한 관리 방안 부재
- 취급위탁 사업자(수탁자)에 대한 실사 미실시



개선방안

- 위탁 사업자(수탁자)에 대한 관리 방안 마련 (내부관리계획)
- 위탁 사업자(수탁자)에 대한 현장 점검 실시

3. 공통된 오류 사례와 개선방안

만 14세 미만 아동정보 수집 시 부족한 요소들!

✖
만 14세 미만 아동 개인정보 수집

부모님의 정보를 입력하시고 확인을 누르세요.

부모 이름

부모 주민등록번호 -

! 고객님의 개인정보는 암호화 되어 처리되며, 설명인증기관 및 아동통신사의 본인확인용으로만 사용됩니다.

☐ 어린이/학생 회원의 부모(법정대리인)임을 확인합니다.

✓ 확인
✕ 취소

- 부모성명 및 주민번호만으로 인증 -



공통 오류내용

만 14세 미만 아동정보 수집 시 법정 대리인의 미동의 및 동의절차 미흡

- 아동정보 수집 시 법정대리인의 동의 절차 미적용
- 법정대리인 동의 시 단순 동의(체크박스) 형태로 운영



개선방안

- 적절한 법정대리인 동의 방식 도입
(ex : 휴대전화, 공인인증서, 신용카드 인증 등)

부모동의 01 약관동의 > 02 본인확인 > 03 부모동의 > 04 개인정보 정책 > 05 가입완료

만 14세 미만 어린이/학생 회원은 부모님과 함께 가입해 주셔야 하며 부모님의 수단을 이용해 가입하실 수 있습니다.

신용카드	휴대폰	범용 공인인증서
부모 명의의 신용카드를 가입하실 수 있습니다.	부모 명의의 휴대폰으로 인증번호를 전송받아 가입하실 수 있습니다.	부모 본인 공인인증서를 가입하실 수 있습니다. (은행, 증권 등 인증서 사용 불가)
> 인증하기	> 인증하기	> 인증하기

[✕ 가입취소](#)

3. 공통된 오류 사례와 개선방안

결혼중개업체는 왜 만14세 미만 아동의 개인정보를 수집할까?

**타사의 개인정보 처리방침을
복사하여 사용한 사례**

OO 결혼정보회사 개인정보 처리방침

- 회원관리
- 회원제 서비스 이용 및 제한적 본인 확인제에 따른 본인확인, 개인식별, 불량회원(기본약관 제9조 2항 및 3항 의 사유로 계약 해지된 회원)의 부정
- 이용방지와 비인가 사용방지, 가입의사 확인, 가입 및 가입횟수 제한, 만14세 미만 아동 개인정보 수집 시
- 분쟁 조정을 위한 기록보존, 불만처리 등 민원처리, 고지사항 전달

이용약관
4. 전자파해제 위한 설계
5. 마일리지 등 "사이트"가 지급한 포인트에 의한 결제
6. "사이트"와 계약을 맺었거나 "사이트"가 인정한 상품권에 의한 결제
7. 기타 전자적 지급 방법에 의한 대금 지급 등
제12조(수신확인통지와국외신상 변경 및 취소)
☒ 약관에 동의합니다.

개인정보 수집 및 이용에 대한 안내
다. 수집한 개인정보의 보유 및 이용기간
회원에 가입한 후에 탈퇴 요청이 있기 전까지 개인정보를 보호합니다.
탈퇴요청이 있다면 회원 탈퇴처리를 하고 탈퇴요청자에게 통보와 동시에 정보는 모두 삭제합니다.
☒ 개인정보 수집 및 이용목적에 동의합니다.



공통 오류내용

타사 개인정보 처리방침 복사 후 사용

- 해당 기업과 맞지 않는 처리방침 내용
(ex : 결혼중개업체가 만14세 미만 아동의 개인정보 수집, 고지 내용과 수집항목의 불일치 등)



개선방안

- 개인정보 처리방침 작성 시 기업 현황 반영
- 내부관리계획을 기반으로 한 개인정보 처리방침 작성

3. 공통된 오류 사례와 개선방안

개인정보 처리방침에 누락된 것은?



개인정보 처리방침 고지의 부적절한 예

▶ 수집하는 개인정보의 항목 4.10P

회사는 회원가입, 상담, 서비스 신청 등등을 위해 아래와 같은 개인정보를 수집하고 있습니다.

- 수집항목: 이름, 생년월일, 성별, 로그인ID, 비밀번호, 자택 전화번호, 자택 주소, 휴대전화번호, 이메일, 결혼여부, 기념일, 주민등록번호, 신체정보, 서비스 이용기록, 접속 로그, 쿠키, 접속 IP 정보
- 개인정보 수집방법: 홈페이지(회원가입, 상담제시판,예약제시판), 전화/팩스를 통한 회원가입, 생체 정보 수집 등을 통한 수집

▶ 개인정보의 수집 및 이용목적 4.10P

회사는

- 서비스 제공
- 회원 관리
- 마케팅 및 광고에 활용

이벤트 등 광고성 정보 전달, 인구통계학적 특성에 따른 서비스 제공 및 광고 게재, 접속 빈도 파악 또는 회원의 서비스 이용에 대한 통계

고지내용 중 개인정보 보호 담당자, 위탁, 제3자 제공 내용 등 미고지

▶ 개인정보의 보유 및 이용기간 4.10P

합법적으로 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체 없이 파기합니다. 단, 관계법령의 규정에 의하여 보존할 필요가 있는 경우 회사는 아래와 같이 관계법령에서 정한 일정한 기간 동안 회원정보를 보관합니다.

- 보존 항목: 이름, 생년월일, 성별, 로그인ID, 비밀번호, 자택 전화번호, 자택 주소, 휴대전화번호, 이메일, 결혼여부, 기념일, 주민등록번호, 신체정보, 서비스 이용기록, 접속 로그, 쿠키, 접속 IP 정보
- 보존 근거: 신용정보의 이용 및 보호에 관한 법률
- 보존 기간: 3년



공통 오류내용

개인정보 처리방침 내 필수항목 누락 및 오류

- 변경사항(ex. 개인정보 보호담당자 퇴사 후) 미반영
- 개인정보 수집 항목과 고지 내용의 불일치
- 제3자 제공 고지 항목과 실제



개선방안

- 개인정보 처리방침 내용 중 필수 고지내용 점검
- 개인정보 수집 항목 및 목적, 제공업체 및 목적, 개인정보 보호 담당자 변경 시 변경 내용 반영

개인정보 처리방침 필수 포함항목

1. 개인정보의 처리목적, 수집 항목
2. 개인정보의 처리 및 보유기간
3. 개인정보의 제3자 제공
4. 개인정보 처리의 위탁 관련 사항
5. 정보주체의 권리 의무 및 그 행사방법

3. 공통된 오류 사례와 개선방안

개인정보를 어떻게 파기하고 있나요?

無

개인정보 파기대장



공통 오류내용

목적달성 또는 계약 종료로 개인정보를 파기할 경우, 이에 대한 절차 및 관리 부재

- 개인정보 파기 매뉴얼 부재
- 개인정보 파기 관리 대장 부재



개선방안

- 내부관리계획을 기반으로 한 개인정보 매뉴얼 작성
- 개인정보 파기 관리대장 기록 및 관리



개인정보 파기 관리 대장 샘플

개인정보 파기 관리대장				
순번	개인정보 내역	보유기간	파기일자	개인정보 확인
1				분쇄(증거사진 첨부)
2				소각(증거사진 첨부)
3				

3. 공통된 오류 사례와 개선방안

개인정보 암호화는 선택사항이 아닙니다.

無

개인정보 암호화 조치



공통 오류내용

수집된 개인정보 중 비밀번호, 고유식별정보, 금융정보 등에 대한 암호화 미조치

- 업무의 효율성 저하로 암호화 미적용



개선방안

- 개인정보 유출사고에 대비해 비밀번호, 고유식별정보에 대한 암호화 조치 수행
- 영세 사업자 경우, 한글, MS 오피스 등의 파일 암호화 기능을 활용해 개인정보 암호화 조치 수행

3. 공통된 오류 사례와 개선방안

우리에게 내부관리계획은 없다!

無

개인정보 보호 내부관리계획



공통 오류내용

기업 고유의 내부관리계획 부재

- 일부 대기업 이외에는 내부관리계획을 수립해 적용하고 있는 곳은 없음
- 이것은 개인정보 수집 및 목적, 이용, 제공, 파기에 이르는 일련의 체계가 없다는 것을 의미



개선방안

- 개인정보 보호 담당자 및 책임자 지정을 시작으로 기업 내 개인정보 흐름 파악
- 관리적·기술적·물리적 보호조치 수행을 위한 계획 수립 및 적용
- 수립된 계획의 운영 여부에 대한 지속적인 점검 및 갱신
- 행안부 및 KISA의 내부관리계획 샘플(배포용) 참고

Thank you



행정안전부



한국인터넷진흥원