

개인정보 위반 사례와 현장 점검결과

2014. 6



안전행정부



한국정보화진흥원

목차

I. 개요

II. 처리단계별 주요 위반 사례

III. '12-'13년 현장점검 결과

IV. 사업자의 조치사항 및 자세

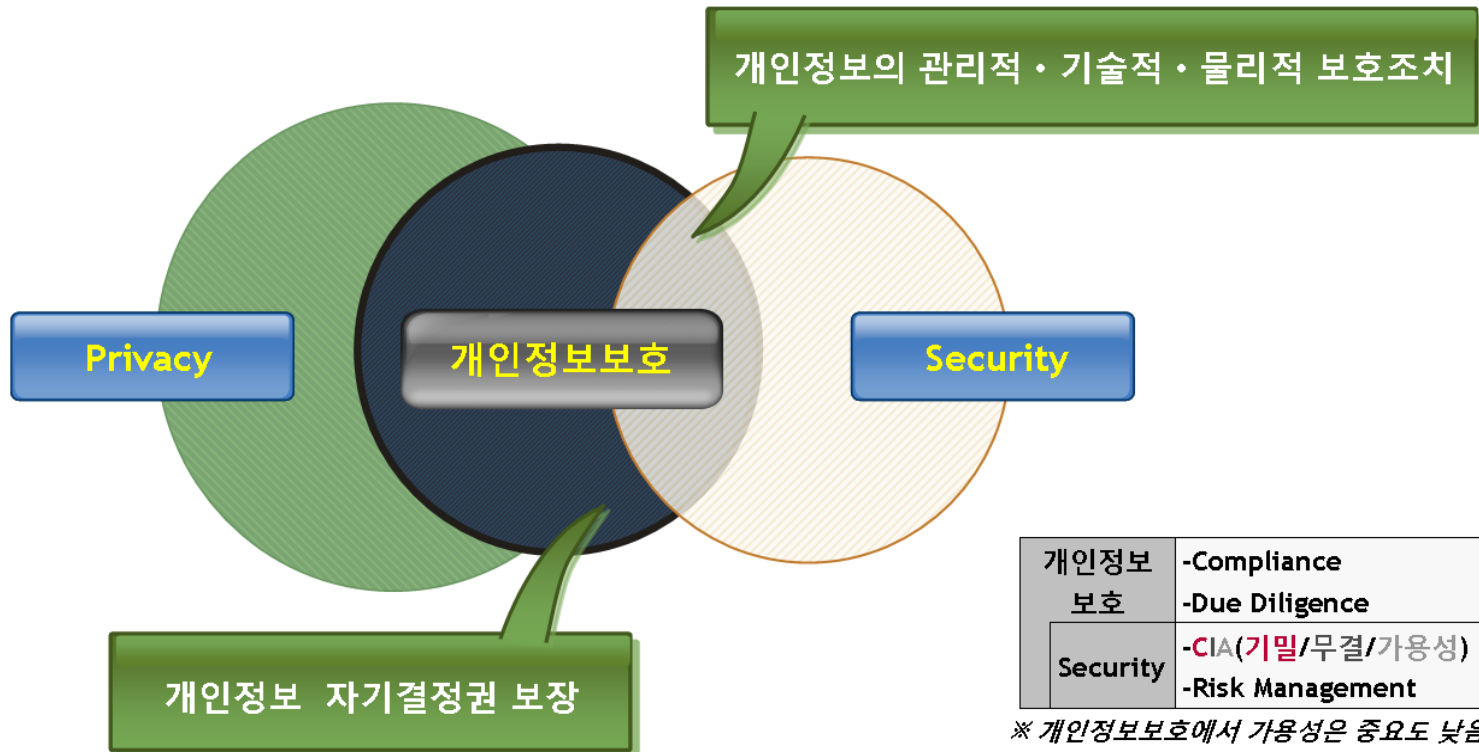
I. 개요

정의

“개인정보”란 살아 있는 개인에 관한 정보로서 성명·주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

- 개인정보보호법 제2조제1항 -

개인정보 보호 요요



※ 개인정보보호에서 가용성은 중요도 낮음

※ 헌법 제17조: 모든 국민은 사생활의 자유와 비밀을 침해 받지 아니한다.

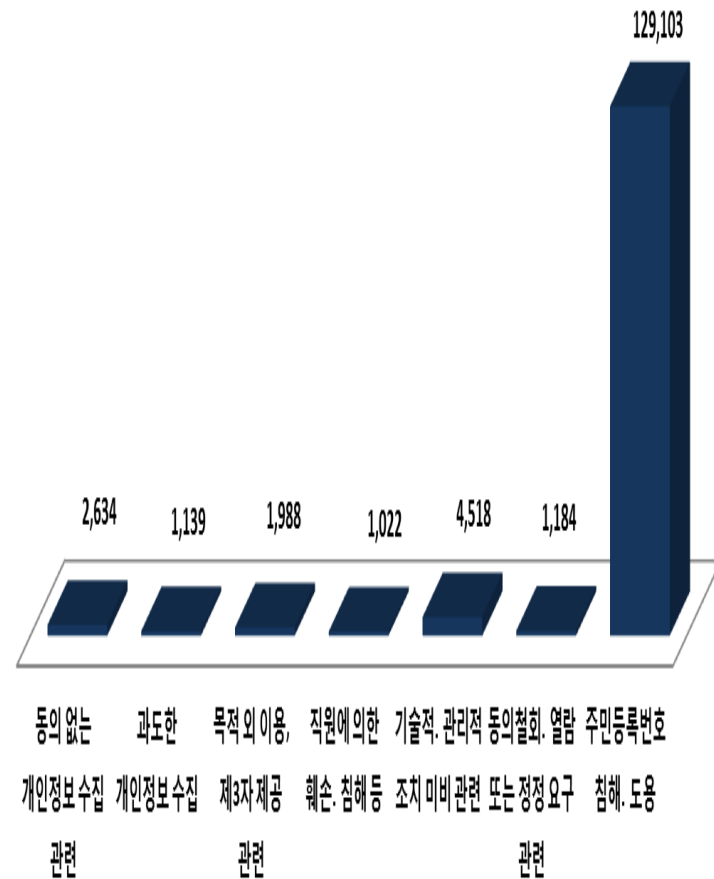
● 개인의 사적 영역과 관련된 일체의 정보 ●



개인정보 침해 민원 현황



침해 유형별 현황(2013)



출처: 개인정보침해신고센터

II. 주요 위반 사례

수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

개인정보 수집 · 이용 시 동의 (위반 사례)



멤버십 가입 신청 시, 수집 · 이용 목적, 수집 항목, 보유 · 이용 기간 등
동의를 받아야 하는 항목 중 일부 누락



호텔

멤버십 가입 신청서



기존 업무관행에 의해
제공 받는 자, 이용목적,
제공 항목, 보유·이용 기간,
동의거부 권리 등을
고지하지 않고 동의획득



멤버십 신청자

수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

개인정보 수집 · 이용 시 동의 (참고 사례)



개인정보 수집에 필요한 고지사항을 모두 고지하고 정보주체의 동의 획득

개인정보처리자

수집 항목

수집 · 이용 목적

보유 · 이용 기간

동의 거부 권리
(신규 추가 사항)

본인이 000000(이하 '회사'라 한다) 인터넷 회원
귀사에 패밀리회원 가입과 관련하여 제공한 아래의 개인정보를 회사에 동의합니다.

위: 이름, 주민등록번호, 아이디(ID), 주소, 연락처, 이메일 주소, 이메일 수신 여부,
수집하지 않습니다.

회원가입 시 회사가 수집하는 정보

2. 정보의 이용목적: 회원 가입 및 서비스 제공을 위하여
3. 정보의 보유 및 이용기간: 회원의 회원정보 변경 또는 회원탈퇴 시 까지
4. 추가정보 제공을 원하지 않는 경우 수집하지 않으며, 미동의로 인해 이용 상의 어떤 불이익도 발생하지 않습니다.

☐ 개인정보제공을 위한 동의서에 동의함 ☒ 동의안함

수집
이용

저장
관리

제공
위탁

파기

권익
보호

2

만14세 미만 아동정보 수집 시 법정 대리인 동의 (위반 사례)



하교하는 아동을 대상으로 이름, 학년, 반, 전화번호, 부모 연락처, 직업 등의 개인정보를 법정대리인 동의 없이 수집

‘이름이 뭐니?’
‘집 전화번호는 뭐니?’
‘부모님 뭐하시니?’

법정대리인 동의 없이
아동의 개인정보 수집



학원 관계자

지속적인
학원 홍보 전화



학교



아동



아동의 부모

수집
이용

저장
관리

제공
위탁

파기

권익
보호

2

만14세 미만 아동정보 수집 시 법정 대리인 동의 (참고 사례)



만14세 미만 아동의 개인정보 수집 시 공인인증서, 휴대폰 인증, 전자우편 등의 방법을 통하여 법정대리인의 명시적 동의 획득

○ 만14세 미만 보호자 동의

★ HOME > 회원



14세 미만은 **보호자의 동의**가 필요합니다.

14세 미만의 학생은 법정 대리인의 동의를 통해서 정식 회원으로 가입하여 서비스를 이용하실 수 있습니다.

보호자의 이름, 주민번호, 휴대폰 번호를 입력 후 휴대폰으로 전송받은 인증번호를 입력해주시기 바랍니다.

만14세 미만 아동에
대한 별도 개인정보
수집 메뉴 개설

휴대폰, 공인인증서,
전자우편 등을 통해
법정대리인 동의 획득

· 방법1 : 보호자 휴대폰 인증



보호자의 휴대폰을
이용하여 인증받기

▶ 휴대폰 전송받기

· 방법2 : 팩스 인증



만14세미만 회원가입
동의를 작성 후
팩스 보내기
(FEX 00-0000-0000)

▶ 동의를 작성 후 팩스 보내기

· 방법3 : 이메일 인증



만14세미만 회원가입
동의를 작성 후
이메일 보내기
(0000@000.000)

▶ 동의를 작성 후 이메일 보내기

수집
이용

저장
관리

제공
위탁

파기

권익
보호

3

민감정보 수집 제한 (위반 사례)



이동통신사가 요금감면을 위해 민감정보(신체 장애 정보)를 수집하면서
정보주체의 동의 미획득

신체 장애,
병력(病歷) 정보



이동통신사 고객

1 요금감면 신청

2

민감정보 수집에 대한
동의 미획득



이동통신사

수집
이용

저장
관리

제공
위탁

파기

권익
보호

3

민감정보 수집 제한 (참고 사례)



민감정보에 대한 수집 · 이용 목적, 수집 항목, 보유 · 이용 기간, 이용자 권리를 별도로 고지하고 별도의 동의 획득

개인정보 수집동의

- 개인정보의 수집 및 이용 목적
 - 회원관리 및 결혼 서비스에 관한 상담 및 자료요청 확인
 - 결혼 관련 서비스 상담
- 수집하는 개인정보의 항목
 - 성명, 아이디, 비밀번호, 휴대폰번호, 이메일 거주지 주소
- 이용 및 보유 기간

민감정보 수집에
대한 별도동의 획득

☐ 동의함

☐ 동의하지 않음

민감정보 수집동의

- 민감정보 수집 목적
 - 결혼상대 추천 시 추가 서비스 제공
 - ** 정보 주최 이벤트 정보 제공
- 수집하는 민감정보 항목
 - 신체정보, 학력, 종교
- 이용 및 보유 기간
 - 회원 탈퇴 시까지 보유

민감정보 수집 항목

☐ 동의함

☐ 동의하지 않음

수집
이용

저장
관리

제공
위탁

파기

권익
보호

4

불필요한 개인정보 과다 수집 (위반 사례)



정유사에서 멤버십 카드 가입을 위해 개인정보를 수집하면서 군 복무 정보를 필수항목으로 요구하고, 미 기재 시 멤버십 가입 불허



정유사



멤버십 카드
신청서 배부

- 필수입력항목에 멤버십과 무관한 “군복무 여부”포함
- 기재하지 않을 경우 멤버십 가입 불허



멤버십 카드
신청 고객

수집
이용

저장
관리

제공
위탁

파기

권익
보호

4

불필요한 개인정보 과다 수집 (참고 사례)



회원 가입 시 수집하는 개인정보를 '**필수**'와 '**선택**' 사항으로 구분하고,
선택사항은 입력하지 않아도 회원가입 허용

정보입력

* 필수입력사항

- * 아이디
- * 비밀번호
- * 성명
- * 휴대폰 번호

**필수사항
입력만으로
회원가입 가능**

* 비밀번호 확인

비밀번호 재발급을 받거나 ID를 찾기 위해서는 휴대폰 번호가 반드시 필요합니다.

추가정보입력

여권유무 ☐ 있음 ☒ 없음 여권번호 여권만료일 (예) 2004-01-01

비자유무 [미국비자]비자번호 비자만료일 (예) 2004-01-01
[일본비자]비자번호 비자만료일 (예) 2004-01-01

생년월일 [1900] 년 [01] 월 [01] 일 ☒ 양력 ☐ 음력

결혼여부 ☒ 미혼 ☐ 기혼 결혼기념일 [1960] 년 [01] 월 [01] 일

수집
이용

저장
관리

제공
위탁

파기

권익
보호

5

수집 · 이용 목적 외 이용 금지 (위반 사례)



보험 서비스를 제공할 목적으로 보험가입자의 개인정보를 수집하였으나,
정보주체의 동의 없이 보험상품 홍보 및 판매를 위해 개인정보 이용



보험회사

1

보험서비스 제공 목적으로
개인정보 수집 동의

2

별도의 보험 대출상품 마케팅



보험가입고객

수집
이용

저장
관리

제공
위탁

파기

권익
보호

5

수집 · 이용 목적 외 이용 금지 (참고 사례)



당초 동의 받은 목적 외에 이벤트 등 다른 목적으로 개인정보 이용 시,
변경된 수집 · 이용 목적, 수집 항목, 보유 · 이용기간 등 재고지 및 동의 획득

□ 경품이벤트를 위한 개인정보 수집 · 이용

이벤트에 대한
수집·이용 목적 등을
고지·동의 획득

- 개인정보의 수집 · 이용 목적 : 경품 당첨시 본인확인 및 경품배송 목적
- 수집하는 개인정보의 항목 : 성명, 주민번호, 휴대전화번호, 주소
- 개인정보의 보유 및 이용 기간 : 이벤트 종료시(경품당첨 및 배송완료 후)

☐ 동의 ☐ 동의하지 않음

수집
이용

저장
관리

제공
위탁

파기

권익
보호

6

개인정보 수집 시, 별도 동의 (참고 사례)



개인정보 수집 시, 필수항목과 선택항목, 고유식별정보, 민감정보, 제3자 제공 등에 대하여 반드시 별도로 고지하고 별도로 동의 획득

A사의 개인정보 수집 및 이용

회사는 회원가입, 고객상담, 서비스 제공을 위해 최초 회원가입 시 아래와 같은 개인정보를 수집하고 있습니다.

<필수정보> 성명, 생년월일, 성별, 아이디, 비밀번호, 필수연락처, 가입인증정보

수집한 개인정보는 회원 유지기간 및 A/S 기간동안 보관합니다.

회원께서는 개인정보 수집 동의를 거부하실 수 있으며 다만 이 경우 회원가입이 제한됩니다.

개인정보 수집 및 이용에 동의하십니까

☐ 동의함

☐ 동의하지 않음

일반동의

(필요시) 고유식별정보 처리 동의 (수집 또는 제공시의 고지사항 고지)

고유식별정보 처리에 동의하십니까

☐ 동의함

☐ 동의하지 않음

별도동의

(필요시) 민감정보 처리 동의 (수집 또는 제공시의 고지사항 고지)

민감정보 처리에 동의하십니까

☐ 동의함

☐ 동의하지 않음

별도동의

(필요시) 목적 외 제공 동의시 (목적 외 제공시의 고지사항 고지)

개인정보 목적외 이용에 동의하십니까

☐ 동의함

☐ 동의하지 않음

별도동의

<선택정보> 기혼 여부, 기념일, 병력, 취미, 소득수준, 자녀 정보

※ 선택정보 사항을 획득하지 못한 사유로 인해 서비스 제공을 거부할 수 있습니다.

선택적 개인정보 수집 및 이용에 동의하십니까

☐ 동의함

☐ 동의하지 않음

별도동의

수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

개인정보보호책임자 지정 (위반 사례)



퇴직한 K씨를 개인정보보호책임자로 계속 방치

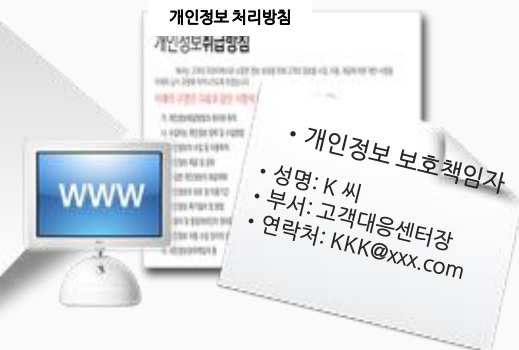


여행사

1 개인정보 보호책임자 K씨 퇴직



2 개인정보 처리방침에
퇴직자 K씨가 계속
보호책임자로 기재
(보호책임자 미지정)



1

개인정보보호책임자 지정 (참고 사례)



전임자 퇴직 시 지체 없이 내부 인사발령 절차를 거쳐 고충처리 담당부서의 장을 개인정보보호책임자로 지정

주식회사 ○○○○

보 존 년 한	1, 3, 5, 10년 영구	인사발령				회 장	
기 안 일 자	2010. 1. 5.					(품 의) / 보 고	
기 안 부 서	홍보마케팅팀	결	달 달 자	일 일 장	이 사	인사발령서	
기 안 자	○○○	재	76	○○○	○○○		
최 종 결 정	가. 부. 보류 인						
지시사항 및 합의의견							
제 목	개인정보 관리 책임자 변경의 건						

상기 건을 다음과 같이 진행하고자 합니다.

- 사 유
· 조직개편 및 인사이동에 따른 개인정보 관리 책임자 변경
- 변경 일자 : 2010. 1. 5.
- 개인정보 관리 책임자 변경
변 경(정)
기획팀 ○○○ 팀장 홍보마케팅팀 ○○○ 팀장

※당사 사내 개인정보 보호업무 규정에 근거
- 주요 업무 및 인수인계 사항 개인정보 보호업무 규정 참고

- 기 타
- 품의 득 후 당사 홈페이지 내 “개인정보취급방침” 책임자 명 변경. 끝.

인사결정권자의 결재를
받은 후 개인정보보호
책임자로 지정

2

개인정보처리방침 공개 (위반 사례)



인터넷 홈페이지에 개인정보처리방침을 게재하면서 글자 크기 · 색상 등을 활용하여 정보주체가 쉽게 확인할 수 있도록 조치하지 않음



2

개인정보처리방침 공개 (참고 사례)



개인정보처리방침을 홈페이지 또는 사업장 내에 게시하여 정보주체가 쉽게 확인할 수 있도록 공개

[인터넷 홈페이지 첫 화면]



공개사항을
모두 포함

- 01. 개인정보의 수집합의
- 02. 개인정보의 수집방법
- 03. 수집한 개인정보의 이용 및 제3자 제공
- 04. 개인정보취급 업무의 위탁
- 05. 개인정보의 보관기간 및 이용기간
- 06. 개인정보의 파기절차 및 방법
- 07. 이용자 및 법정 대리인의 권리와 그 행사방법
- 08. 개인정보의 자동 수집 장치의 설치, 운영 및 그 동의 거부할 수 있음에 관한 사항
- 09. 개인정보취급방침의 고지 또는 통지방법
- 10. 개인정보보호를 위한 기술적·관리적 대책
- 11. 개인정보관리책임자 및 담당자
- 12. 이동의 개인정보보호

[사업장내 벽면에 게시]



정보주체가 쉽게
확인할 수 있도록
글자색을 달리 표시

약관 개인정보 처리방침 회사소개/투자정보 온라인제휴안내

수집
이용

저장
관리

제공
위탁

파기

권익
보호

3

개인정보 내부관리계획 수립 · 시행 (참고 사례)



개인정보 내부관리계획을 수립하고 조직 내 의사결정자(CEO, CPO, 담당
임원 등)의 결재를 거쳐 시행

개인정보 관리계획서

목 차

- I. 목 적
- II. 적용근거
- III. 범위

의사결정자 결재를
거쳐 내부관리계획
수립·시행

- IV. 작성프로그램 명칭
- V. 수집·처리지 보유조치
- VI. 개인정보 표시 제한 보유조치
- VII. 기업정보의 이용제한 및 파기

*별첨·가입자 참조



목적

적용근거

적용범위

개인정보보호 조직

개인정보보호 교육

접근통제

위탁업체 관리

침해대응

내부 감사

개인정보의 수집

아동의 개인정보보호

이용 및 제공

제3자 제공

개인정보 파기

내부관리계획의 승인 및 검토

수집
이용

저장
관리

제공
위탁

파기

권익
보호

4

개인정보 접근권한 관리 (위반 사례)



퇴직한 직원의 접근권한을 변경하지 않아, 퇴직한 직원이 개인정보처리 시스템에 접근하여 개인정보 유출



퇴직자

1

쇼핑센터 재직 시 사용하던 ID/PW로 접근 시도

2

개인정보 처리시스템에 접근 후 고객명부 불법 탈취

3

경쟁업체에 고객명부 판매



경쟁업체



쇼핑센터

수집
이용

저장
관리

제공
위탁

파기

권익
보호

5

개인정보 암호화 조치 (위반 사례)



주민등록번호, 비밀번호 등을 암호화하지 않아 해킹으로 유출

해커

1 해킹 시도



리조트

3 개인정보 판매

2 암호화 되지 않은
회원의 주민등록번호, 비밀번호 유출



불법 개인정보
구매자

홍길동	601111-1234567
김순돌	420112-2345123
...	781230-2345123
...	801231-2011111

수집
이용

저장
관리

제공
위탁

파기

권익
보호

6

보안 프로그램의 설치 · 운영 (위반 사례)



개인정보처리시스템 운영체제에 최신 보안패치를 업데이트하지 않아
외부 공격자(해커) 보안취약점을 이용하여 개인정보 유출



공격자

1 운영체제 보안취약점을 이용한 해킹

2 관리자 권한 획득으로
개인정보 파일 빼냄



결혼중개업

3 개인정보 판매



K씨

업데이트
미적용



개인정보처리시스템

수집
이용

저장
관리

제공
위탁

파기

권익
보호

7

개인정보처리시스템 접속 기록 보존 (위반 사례)



내부직원에 의해 개인정보가 유출되었으나, 개인정보 접근사실을 기록하지 않아 유출자 확인 불가능



1

개인정보처리시스템에 접속하여
고객 개인정보 조회·유출



내부 직원

2

접속기록 미보관

ID	Name	Access Date	Access Time	Access IP	Access User	Access Method	Access Result	Access Detail
1001	김민준	2014-01-15	10:00:00	192.168.1.100	admin	SQL	Success	SELECT * FROM CUSTOMER
1002	이성민	2014-01-15	10:05:00	192.168.1.101	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1001
1003	박지민	2014-01-15	10:10:00	192.168.1.102	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1002
1004	정지민	2014-01-15	10:15:00	192.168.1.103	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1003
1005	최지민	2014-01-15	10:20:00	192.168.1.104	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1004
1006	김민준	2014-01-15	10:25:00	192.168.1.100	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1005
1007	이성민	2014-01-15	10:30:00	192.168.1.101	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1006
1008	박지민	2014-01-15	10:35:00	192.168.1.102	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1007
1009	정지민	2014-01-15	10:40:00	192.168.1.103	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1008
1010	최지민	2014-01-15	10:45:00	192.168.1.104	admin	SQL	Success	SELECT * FROM CUSTOMER WHERE ID=1009



8

홈페이지를 통한 개인정보 노출 (위반 사례)



개인정보취급자(또는 안내원)의 실수로 타인이 볼 수 있는 홈페이지 Q&A 게시판에 고객 상세정보 노출



L씨

1

자신의 정보에 대한 질문 글을
게시판에 게재



쇼핑센터

2

개인정보 내용이 담긴
답글을 Q&A게시판에 공개



3

다른
이용자까지
L씨의 정보
확인

수집
이용

저장
관리

제공
위탁

파기

권익
보호

9

검색엔진을 통한 개인정보 노출 (위반 사례)



홈페이지의 잘못된 설정으로 사업자의 개인정보 데이터가 검색로봇 또는 검색사이트를 통해 검색결과로 노출

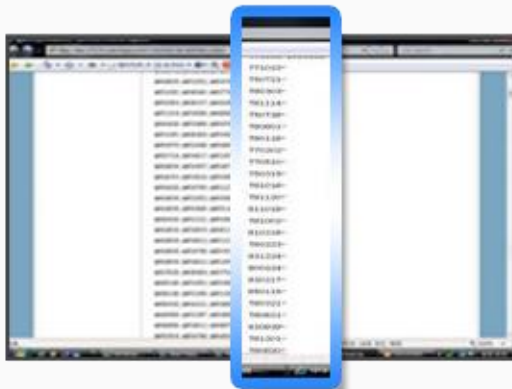


A기관

1 검색로봇 배제 옵션 미설정



2 검색사이트에
A 기관 DB 검색



3 주민번호가
검색결과로 노출



10

CCTV 등 영상처리기기 적법 운영 (위반 사례)



영상처리기기(CCTV) 설치·운영 시 단순 영상 녹화기능 뿐만 아니라,
음성녹음 기능을 사용해 목적 이외의 정보 수집



1 영상정보 녹화



정보주체

2 영상 및 음성 정보까지
녹화 및 수집



관리자

수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

제3자 제공 시 동의 (위반 사례)



대형마트가 경품행사에 응모한 정보주체의 개인정보를 동의 없이
생명보험사에 제공



1 물품구입 후 받은 응모권으로
경품행사 참여



대형 마트

2

동의 없이
고객정보 제공



생명보험사



마트 고객

3 보험상품 홍보전화

수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

제3자 제공 시 동의 (참고 사례)



백화점이 보험업체와의 마케팅 제휴를 통해 회원 개인정보 제공 시, 제공받는 자, 제공 목적, 제공 항목 및 이용 기간 등을 명시하고 별도 동의 필수

3 보험상품 홍보전화



생명보험사

동의
획득
방법

2 동의 획득 후
고객정보 제공



백화점 고객

1 회원가입 시
개인정보제공 동의 백화점



개인정보 수집 · 이용 동의

주식회사 00000은 인터넷 웹사이트에서의 개인정보보호를 매우 중요하게 생각 하며, 회원님의 사생활에 관련된 정보를 보호하고, 불법적인 개인정보 유출 및 피해를 방지하도록 최선의 노력을 다하겠습니다.
현대백화점 회원의 개인정보보호 정책은 '정보통신망이용촉진 및 정보보호에 관한 법률'상의 개인정보보호규정 및 정보통신부가 제정한 '개인정보보호지침'을 준수하고 있으며, 본 정보통신망에서 저장한 개인정보보호지침 제7조에 의거하여 개인정보보호정책

☒ 동의합니다. ☐ 동의하지 않습니다.

개인정보 제공 및 활용 동의서

주식회사 00000은 인터넷 웹사이트에서의 개인정보보호를 매우 중요하게 생각 하며, 회원님의 사생활에 관련된 정보를 보호하고, 불법적인 개인정보 유출 및 피해를 방지하도록 최선의 노력을 다하겠습니다.
00000 00000 00000 00000
· 이용 목적 : 보험판매 등의 TM
· 제공 정보 : 이름, 주민번호, 자택주소, 자택전화, 휴대폰
· 정보 이용 및 보유기간 : 현대백화점 회원 활동 또는 제휴계약 종결 시 까지

별도동의

개인정보 제공
현황고지

☒ 동의합니다. ☐ 동의하지 않습니다.

수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

제3자 제공 시 동의 (참고 사례)



여행서비스를 위해 항공사 등에 개인정보를 제공하는 경우, 제공받는 자, 제공받는 자의 이용목적, 제공항목 및 보유·이용기간을 고지하고 동의획득

제공받는 자

00000, 00000000 및 국내외 제휴항공사, 국내외 호텔 및 숙박업체, 철도, 크루즈 및 운송업체, 해외 렌드사

제공 항목

영문성명, 생년월일, 여권번호, 여권만료일, 성명, 주민번호, 마일리지정보, 회원등급

제공받는 자

제공받는 자의
이용 목적

항공권 및 기타운송업체 탑승 예약, 숙박예약, 출국가능여부 파악, 현지 행사진행 및 고객관리 목적 마일리지 적립, 전환, 사용, 확인, 회원할인 및 기타의 서비스 제공

00000, 00000, 기타 제휴보험사 외 기타 보험사

성명, 주민등록번호

여행자보험가입, 제휴, 마일리지 적립, 전환, 회원할인 및 기타공

보유·이용 기간

* 보유 및 이용기간: 이용목적에 따른 개인정보 제공시~ 이용목적 달성시 및 관계법령에 따른 보관기간까지 (제휴업체에는 제휴계약 종료시까지)

☐ 동의

☐ 동의하지 않음

수집
이용

저장
관리

제공
위탁

파기

권익
보호

2

홍보 목적의 개인정보 취급위탁 시 동의 (위반 사례)



본래의 서비스 제공 계약과는 관계없는 제휴서비스를 홍보하기 위하여,
텔레마케팅 업무를 콜센터에 위탁하면서 개인정보 처리위탁 사실을 미통지

쇼핑센터



1

업무제휴



B 제휴사



2

취급위탁에 대해 정보주체에게
통지 없이 개인정보 처리를 위탁

콜센터



3

고객에게
통지되지 않은
별도의 제휴
서비스 홍보

고객



수집
이용

저장
관리

제공
위탁

파기

권익
보호

2

홍보 목적의 개인정보 취급위탁 시 통지 (참고 사례)



개인정보 취급 업무 위탁 중 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우 위탁받는 자 및 위탁업무의 내용을 정보주체에게 통지

수집한 개인정보 취급위탁

0000은 서비스 향상을 위해 고객의 개인정보를 외부에 위탁하여 처리하고 있으며, 관계법령에 따라 위탁계약시 개인정보가 안전하게 관리될 수 있도록 규정하고 있습니다. 현재, 개인정보 취급 위탁자와 그 업무의 내용은 다음과 같습니다.

위탁 받는 자

위탁 업무의
내용

위탁자	위탁 업무 내용	제공하는 정보
0000 아이앤씨(주)	고객 상담 업무 일체	- 회원정보, 주문정보
(주) 00 이디에스 (주) 0000 아이앤씨 (주) 000 파트너스 (주) 000 넷 (주) 0000 시스템	전산시스템의 구축 및 유지보수	- 회원정보, 주문정보
00 토사스탁스무역회사, 000 물류, 00 물류업체	상품 배송업무	- 배송정보
00 신용평가정보(주)	실명확인 및 본인인증 등	- 회원정보

수집
이용

저장
관리

제공
위탁

파기

권익
보호

3

개인정보처리 위탁자에 대한 관리·감독 (위반 사례)



IT서비스 운영을 전문업체에 외부 위탁하였으나, 개인정보 취급업무에 대한 관리감독을 수행하지 않아 개인정보 유출



여행사(위탁자)

1

IT서비스 운영위탁 후
관리·감독 미이행



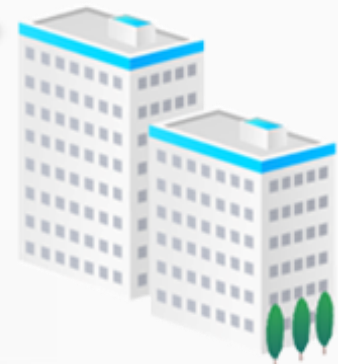
IT 전문업체
퇴직자

2

개인정보처리시스템
접근통제조치 미비

3

재직 시 수집한
개인정보 유출



IT 전문업체
(수탁자)

수집
이용

저장
관리

제공
위탁

파기

권익
보호

3

개인정보처리 위탁자에 대한 관리·감독 (참고 사례)



개인정보 취급위탁 계약서에 위탁자의 개인정보보호조치 등 관련 사항을 명시하고 지속적으로 관리·감독 실시

주식회사 (이하 "을"이라 함)은 2009. 9. 1. (이하 "갑"이라 함)과 체결한 'DM발송시스템 운영 대행 계약' (이하 "본 계약"이라 함)과 관련하여, 본 계약상 "DM발송 시스템"을 이용하는 "갑" 또는 "갑"의 판매위탁대리점, 협력업체 소속 임직원(이하 "이용자"라 함) 및 "갑"의 고객정보를 보호하기 위해 아래와 같이 약정(이하 "본 약정"이라 함)한다.

제 1 조 (개인정보)

본 약정서의 "개인정보"의 의미는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제2조 제6호 정의에 의한다.

제 2 조 (업무목적 외 사용 금지)

- ① "을"은 "갑"이 제공하는 "이용자" 및 고객의 개인정보를 본 계약사항 위탁업무와 직접 관련 된 목적으로만 사용할 수 있고, 이를 제3자에게 임의로 제공하거나 공개할 수 없다.
- ② "을"은 "갑"의 사전 동의없이 전항의 정보를 위탁업무 이외의 목적으로 저장, 출력하거나 복제, 가공할 수 없다.

수탁자가 이행해야 하는 개인정보 보호조치 명시

제 3 조 (개인정보 보호조치)

- ① "을"은 다음 각호의 조치를 구체적으로 마련하여 "갑"에게 서면으로 알려 승인을 받아야 한다.
 1. 개인정보를 관리할 책임자 지정 등 개인정보의 안전한 취급을 위한 내부관리계획
 2. 개인정보를 취급할 수 있는 자(이하 "정보취급자")를 정하는 등 불법적인 접근을 차단하기 위한 조치
 3. 접속기록의 위·변조를 방지하기 위한 조치
 4. 개인정보가 안전하게 저장·전송될 수 있도록 보안조치
- ② "을"은 개인정보 처리에 이용하는 정보기기에 컴퓨터 바이러스, 스파이웨어 등 악성 프로그램의 침투여부를 항상 점검·지료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 경신·점검하여야 한다.
- ③ "을"은 정보취급자에 대한 정기적인 보안교육을 실시해야 한다.

수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

개인정보 파기 (위반 사례)



결혼중개업체가 이벤트 행사 목적으로 수집한 개인정보를 이벤트 종료 후에도 파기하지 않고 홍보 목적으로 이용



P씨

1

이벤트 참여 고객으로부터
개인정보 수집



결혼중개업

2

이벤트 종료 후에도 여행상품 소개
문자메시지 지속 발송



수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

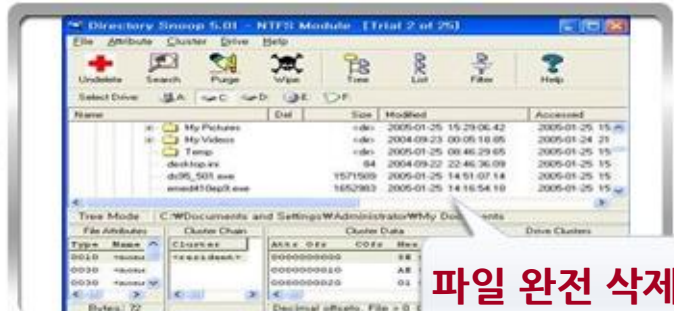
개인정보 파기 (참고 사례)



종이에 출력된 문서는 문서파쇄기로 분쇄하여 파기
전자적 파일형태의 개인정보는 전용 소거 S/W를 사용하여 영구 삭제



분쇄



파일 완전 삭제

수집
이용

저장
관리

제공
위탁

파기

권익
보호

1

정보주체 권리 보호 (위반 사례)



정보주체의 개인정보 이용 동의 철회 및 광고 문자 수신 거부에도 불구하고
광고문자를 수 차례 발송



L씨

1

여행상품 광고 문자메시지
수신거부 요청



여행사

2

여행상품 광고 문자메시지
지속적 발송



수집
이용

저장
관리

제공
위탁

파기

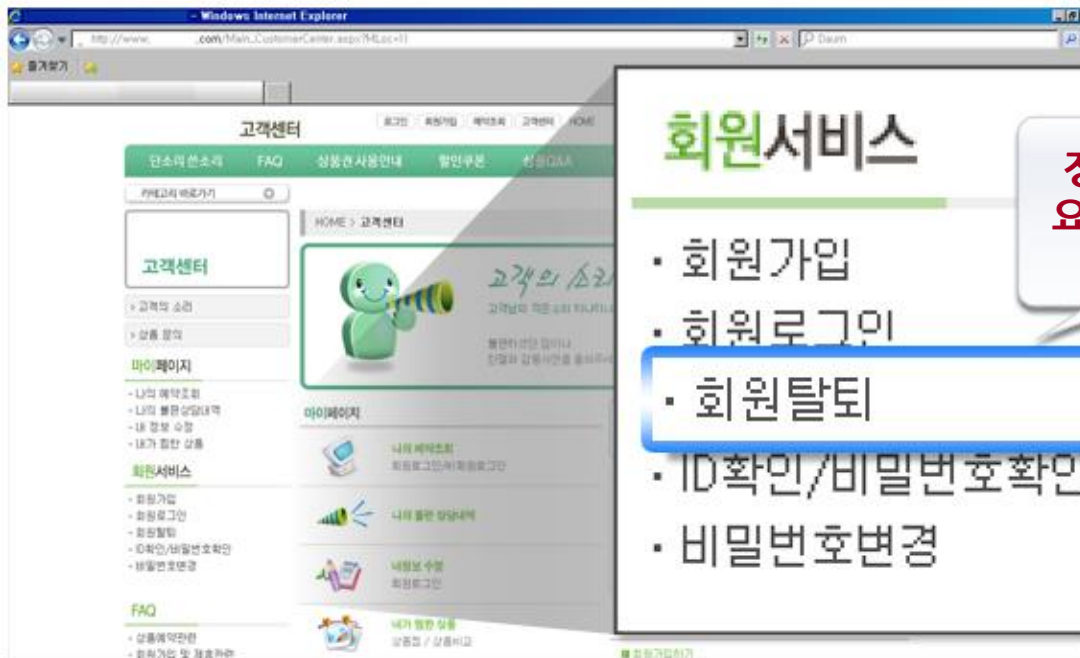
권익
보호

1

정보주체 권리 보호 (참고 사례)



개인정보 수집 방법 보다 쉽게 동의 철회를 할 수 있도록 홈페이지에서 즉시
회원 탈퇴 메뉴 제공



정보주체의 동의철회
요구를 즉시 처리할 수
있도록 메뉴 지원

- 회원가입
- 회원로그인
- 회원탈퇴
- ID확인/비밀번호확인
- 비밀번호변경

Ⅲ. '12-'13년 현장점검 결과

1. 현장점검 개요

조사 및 점검

-기획 점검 : 취약 분야, 위험 업종 대상 중심 실시, 제도개선 병행 (정기)

-특별 점검 : 침해사고, 유출 신고 등 사고 원인조사 및 책임 규명 (수시)



<개인정보보호 합동점검단>



현황 조사분석

- 업종별 개인정보처리현황
- 개인정보관리실태
- 개인정보 제공/활용현황

▶ KISA, NIA, 리서치 등



모니터링

- 개인정보 유/노출현황
- 온라인 점검 (취약점 분석)

▶ 관계부처/기관 연계



침해사고, 민원

- 개인정보 침해신고, 민원
- 분쟁조정 신청
- 사고 발생, 언론 보도 등

▶ 경찰, KISA 등

2. '12~'13년 현장점검결과(1)

행정처분 총괄 현황

- 기획점검 : 자료를 분석하여 침해 우려가 큰 업종으로 대상 선정, 취약점 위주 점검
- 특별점검 : 침해 신고 및 민원 접수, 언론 보도된 기관 등을 대상으로 점검

(단위 : 개소, 건)

구 분	'12년	'13년	합 계
처분기관 수 / 점검기관 수	348 / 423	297 / 331	645 / 754 (85.5%)
행정처분 건수	727	468	1,195
과태료부과(§75)	38	113	151
시정 조치(§64)	342	147	489
개선 권고(§61)	347	208	555

2. '12~'13년 현장점검결과(2)

▣ 위반 주체, 위반 내역 및 조치 내용별 세부 현황

(단위 : 개소, 건)

위반 주체 위반 내역	조치 내용	공공기관				민간사업자			
		과태료	시정 조치	개선 권고	합계	과태료	시정 조치	개선 권고	합계
수집 동의 위반(§15, §17, §22, §23, §24)		4	1	15	20	31	141	88	260
과도한 개인정보 수집(§16, §18)		0	2	0	2	0	11	41	52
침해, 열람 등 위반(§34, §35, §36, §37, §59)		0	1	0	1	1	6	2	9
안전 조치 미흡(§29)		8	12	90	110	36	67	97	200
위·수탁 위반(§26)		7	6	10	23	28	26	2	56
CCTV 설치·운영 위반(§25)		0	9	14	23	23	124	102	249
기타(§21, §28, §30, §31, §32, §33)		0	13	31	44	13	70	63	146
합 계		19	44	160	223	132	445	395	972

3. 개인정보 침해실태('12~'13년6월)

개인정보 생명주기	침해 유형	118 신고 (248,720건)	분쟁조정 (293건)	행정처분 (1,057건)
수집	<ul style="list-style-type: none"> 이용자의 동의 없는 개인정보 수집 과도한 개인정보 수집, 민감한 개인정보 수집 주민등록번호 수집방법 위반, 도용/침해 	<ul style="list-style-type: none"> - 4,848건 - 1,413건 - 202,863건 	<ul style="list-style-type: none"> - 27건 - 6건 - 2건 	<ul style="list-style-type: none"> - 124건 - 53건 - 56건
관리	<ul style="list-style-type: none"> 기술적·관리적 조치 미비로 개인정보 침해 위탁절차 위반 및 위탁업체 관리감독 미흡 	<ul style="list-style-type: none"> - 20,426건 - 149건 	<ul style="list-style-type: none"> - 107건 - 	<ul style="list-style-type: none"> - 265건 - 56건
이용 제공	<ul style="list-style-type: none"> 목적 외 이용 및 동의없는 제3자 제공 접근권한 부실, 부당 공유 및 불법 거래 개인정보 이용 동의 철회 및 회원탈퇴 요구 불응 	<ul style="list-style-type: none"> - 3,107건 - 941건 - 1,642건 	<ul style="list-style-type: none"> - 89건 - 2건 - 9건 	<ul style="list-style-type: none"> · 검거 / 기소 - 1건 - 3건
파기	<ul style="list-style-type: none"> 정당한 이유없는 개인정보 보유 및 미파기 	<ul style="list-style-type: none"> - 1,041건 	<ul style="list-style-type: none"> - 15건 	<ul style="list-style-type: none"> - 10건
기타	<ul style="list-style-type: none"> 개인정보처리방침 누락, 미공개 등 	<ul style="list-style-type: none"> - 12,915건 	<ul style="list-style-type: none"> - 36건 	<ul style="list-style-type: none"> - 206건

〈사례 1〉 물류 및 유통사업자 일제 점검('12. 6월)

배경

- 택배, 백화점, 대형마트 등 물류, 유통업체의 개인정보 침해 위험 증가
- 대상 기관 : ○○택배, ○○백화점, ○○마트 등 6개 사업자
- “행정안전부” 현장 점검 → 과태료 10건(3,200만원), 시정명령 3건

주요위반내용

○ ○○ 택배

- ☐ 위탁계약시 “문서” 에 의한 필수사항 반영 및 조치 미흡
- ☐ 내부관리계획 미수립, 주민번호와 비밀번호의 전송시 암호화 미조치
- ☐ 개인정보 처리방침 중 필수사항 기재 누락

○ ○○ 백화점

- ☐ 주민등록번호 수집에 대한 별도 동의 위반
- ☐ 개인정보처리시스템에 대한 접속기록 관리 위반
- ☐ 선택정보에 대한 필수 수집항목 분류

○ ○○ 마트

- ☐ 위탁계약시 “문서” 에 의한 필수사항 반영 및 조치 미흡
- ☐ 마케팅 목적의 개인정보 수집에 대한 구분 동의 위반

〈사례 2〉 구글링 검색 방식 유출 사고 (‘12. 7월)

배경

- 은둔형 외톨이, 구글링 검색 방식 개인정보 유출 (총 884만 고객정보)
- 대상 기관 : ○○ 공사, ○○ 대학교, ○○ 병원 등 총 14개
- “합동점검단” 현장 점검 → 과태료 18건, 시정명령 2건

주요위반내용

○ ○○ 공사

- ☐ 위탁계약시 “문서” 에 의한 필수사항 반영 및 조치 미흡
- ☐ 송수신/저장 암호화 미조치, 비밀번호 양방향 암호화, 작성규칙 위반 등
- ☐ 유출 통지 절차 위반 및 미 통지 (일부 대상)

○ ○○ 대학교, ○○ 손보사

- ☐ 개인정보처리시스템 접근 권한 공유, 변경 관리 미흡 (부여, 변경, 말소 미조치)
- ☐ 접근기록 관리 미흡, 비밀번호 작성 규칙 위반 등

○ ○○ 병원

- ☐ 접근권한 공유, 비밀번호 작성 규칙 위반 등

〈사례 3〉 보험사 일제 점검 ('12. 8월~9월)

배경

- 온라인 보험사 과도한 고객유치경쟁, 보험관리사 개인정보 취급 부실 등
- 대상 기관 : 생보사, 손보사 등 총 12개사 (보험대리점 포함)
- “점검단” 현장 점검 → 과태료 20건, 시정명령 13건, 제도개선 1건

주요위반내용

- 수집·처리 관련 고지 및 동의 절차 위반 (9개사, 과태료 2,800만원)
 - 고지사항 미안내, 주민번호 수집 및 보험판매 권유를 위한 별도동의 위반
- 수탁사 관리감독 소홀 등 위탁시 준수사항 위반 (4개사, 과태료 800만원)
 - 위탁서 체결시 보호조치사항 미흡, 수탁사 교육·점검 미 실시
- 기술적 보호 등 안전성 확보조치 위반 (6개사, 과태료 3,300만원)
 - 주민번호 암호화 미조치, 접근권한 관리 부실 등

〈사례 4〉 은행권 CCTV 운영실태 일제 점검 (‘12. 11월)

배경

- 은행 ATM기 고객정보 과도한 촬영, 수탁사 부실 관리 등
- 대상 기관 : 총 20 개 은행 (제1, 2 금융권)
- “합동점검단” 현장 점검 → 과태료 19건, 시정명령 7건, 개선권고 3건

주요위반내용

- 전반적으로 CCTV 안내판 설치, 녹음기능 미사용, 전담조직 및 개인정보보호책임자 지정 등은 양호

〈 주요 위반사항 〉

- ① 접근권한 관리 위반(9건), 암호화 미조치(5건), 열람기록 관리 위반(3건)
- ② CCTV 운영업무 위탁처리시 관리·감독 미흡
(위탁계약서상 필수사항 누락, 보호조치 미비 등 4건)
- ③ 개인영상정보(고객의 비밀번호·계좌번호)의 과도한 수집(3건)
- ④ 보유기간이 경과한 영상정보 미파기(3건)

VI. 개인정보보호를 위한 사업자 수칙

개인정보보호를 위한 수칙 (사업자)



- 1 개인정보는 필수정보만 최소한으로 수집
- 2 주민등록번호와 건강정보 등 민감정보 수집 금지
- 3 수집한 목적과 다르게 사용하거나 제3자 제공 금지
- 4 개인정보를 처리할 경우 개인정보 처리방침 공개
- 5 내부관리계획, 방화벽 · 백신 · 접근통제 등 안전성 확보 조치
- 6 개인정보의 이용이 끝난 후에는 반드시 파기
- 7 개인정보가 유출되었을 경우 즉시 정보주체에게 통보
- 8 CCTV를 운영할 경우 안내판을 설치



감사합니다

• 참고자료 : 개인정보보호 종합지원 포털 : www.privacy.go.kr