

개인정보의 안전한 관리 방안

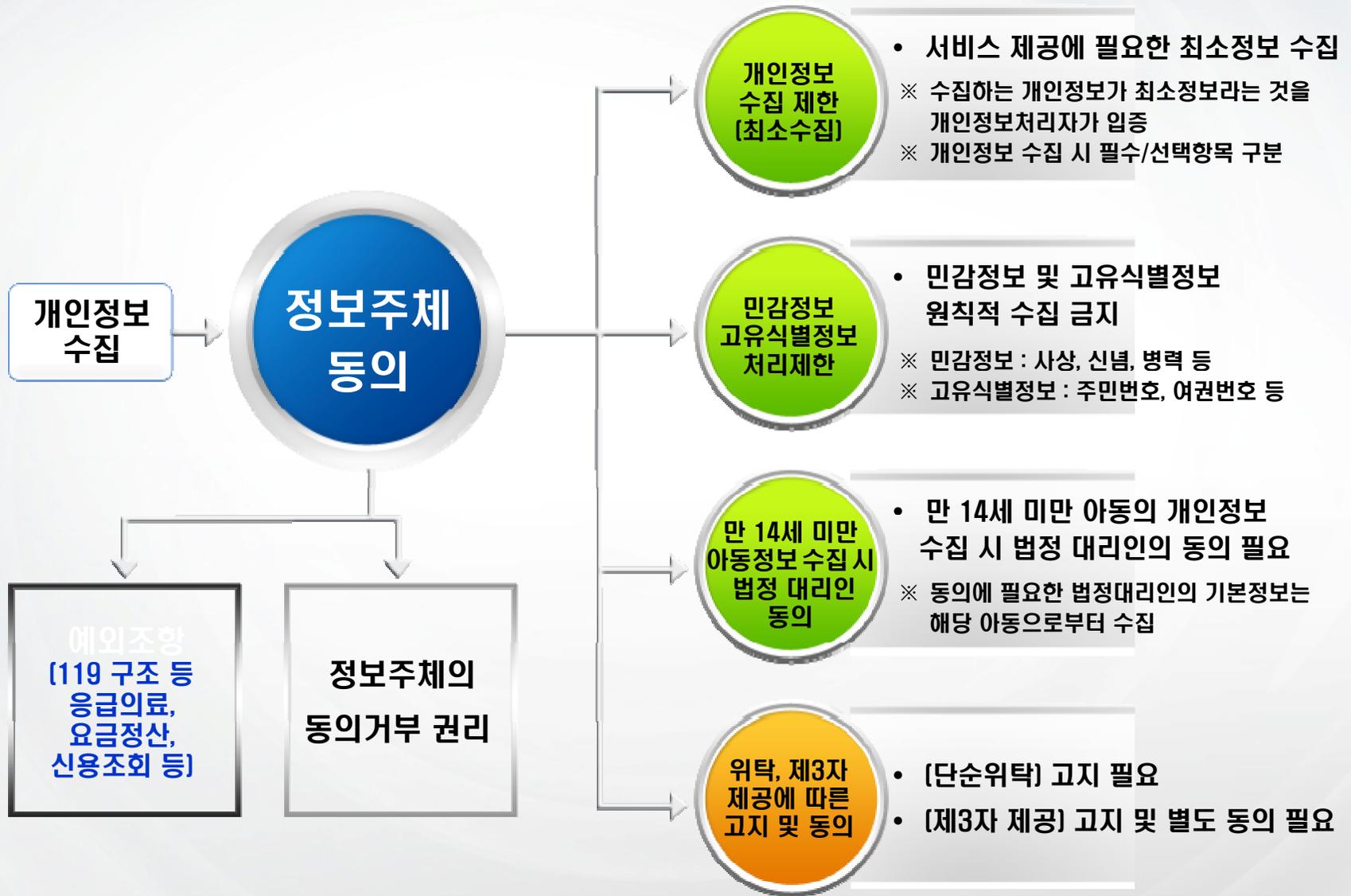
보안전략연구소
박나롱



1-1. 기업 개인정보 보호의 범위



1-2. 수집 및 동의 획득 시 고려사항



1-3. 수집 시 동의획득 항목(수집 및 이용목적)

기업의 개인정보 수집 시 동의획득 항목 예시

개인정보의 수집 · 이용 목적

** 정보(주)는 다음과 같은 목적을 위하여 개인정보를 수집하고 있습니다.

- 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산
[콘텐츠 제공, 특정 맞춤 서비스 제공, 물품배송 또는 청구서 등 발송, 본인인증, 구매 및 요금 결제, 요금추심]
- 회원관리
[회원제 서비스 이용 및 제한적 본인 확인제에 따른 본인확인, 개인식별, 불량회원의 부정 이용방지와 비인가 사용방지, 가입의사 확인, 가입 및 가입횟수 제한, 만14세 미만 아동 개인정보 수집 시 법정 대리인 동의여부 확인, 추후 법정 대리인 본인확인, 분쟁 조정을 위한 기록보존, 불만처리 등 민원처리, 고지사항 전달]
- 신규 서비스 개발 및 마케팅 · 광고에의 활용

개인정보 수집 시 동의획득 항목



1-3. 수집 시 동의획득 항목(수집항목)

기업의 개인정보 수집 시 동의획득 항목 예시

수집하는 개인정보의 항목

****정보(주)는 원활한 서비스 제공을 위해 다음과 같은 항목의 개인정보를 수집하고 있습니다.**

- <실명확인 회원가입 : 주민번호/아이핀 가입>
 - ✓ 필수항목 : 성명, 주민등록번호(아이핀 회원은 생년월일, 성별, 아이핀 번호), 아이디, 비밀번호, 별명, 본인확인문답, 만 14세 미만은 법정대리인 정보, 가입인증정보
 - ✓ 선택항목 : 이메일 주소, 휴대폰 번호
- 서비스 이용과정이나 사업처리 과정에서 아래와 같은 정보들이 자동으로 생성되어 수집될 수 있습니다.
 - ✓ IP Address, 쿠키, 방문 일시, 서비스 이용 기록, 불량 이용 기록

개인정보 수집 시 동의획득 항목



1-3. 수집 시 동의획득 항목(보유 및 이용기간)

기업의 개인정보 수집 시 동의획득 항목 예시

개인정보의 보유 및 이용기간

이용자의 개인정보는 원칙적으로 개인정보의 수집 및 이용목적이 달성되면 지체 없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

- 회사 내부 방침에 의한 정보보유 사유
 - ✓ 부정이용기록
 - ✓ 보존 이유 : 부정 이용 방지
 - ✓ 보존 기간 : 1년
- 관련법령에 의한 정보보유 사유
 - ✓ 본인확인에 관한 기록
 - ✓ 보존 이유 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률
 - ✓ 보존 기간 : 6개월
 - ✓ 웹사이트 방문기록
 - ✓ 보존 이유 : 통신비밀보호법
 - ✓ 보존 기간 : 3개월

개인정보 수집 시 동의획득 항목



1-3. 수집 시 동의 획득 항목(수집 동의 거부 사항)

기업의 개인정보 수집 시 동의 획득 항목 예시

개인정보 수집 동의 거부 권리

****회사는 개인화되고 맞춤형 서비스를 제공하기 위해서 이용자의 정보를 저장하고 수시로 불러오는 '쿠키(cookie)'를 사용합니다. 쿠키는 웹사이트를 운영하는데 이용되는 서버가 이용자의 브라우저에게 보내는 아주 작은 텍스트 파일로 이용자 컴퓨터의 하드디스크에 저장됩니다.**

- **쿠키의 사용 목적**
 - ✓ 이용자들이 사용한 각 서비스와 웹 사이트들에 대한 방문 및 이용형태, 인기 검색어, 보안접속 여부, 뉴스편집, 이용자 규모 등을 파악하여 이용자에게 최적화된 정보 제공을 위하여 사용합니다.
- **쿠키의 설치/운영 및 거부**
 - ✓ 이용자는 쿠키 설치에 대한 선택권을 가지고 있습니다. 따라서 이용자는 웹브라우저에서 옵션을 설정함으로써 모든 쿠키를 허용하거나, 쿠키가 저장될 때마다 확인을 거치거나, 아니면 모든 쿠키의 저장을 거부할 수도 있습니다.

개인정보 수집 시 동의 획득 항목



1-4. 수집 및 이용목적 고지

개인정보 수집 및 이용 목적 변경 시 고지

OOOOO은 이용자 여러분의 개인정보를 무엇보다 소중한 취급하고 있으며,

1. 주요 개정내용

- 개인 정보 수집항목 수정 : 이름 및 주민등록번호 삭제
- 개인정보 제3자 제공 수정 : 실명확인을 위한 이름 및 주민등록번호 제공 중단
- 이용자 및 법정대리인의 권리와 행사방법 규정 병합
- 개인정보 관리 책임자 및 담당자, 청소년 보호 담당자 변경

현행	변경
<p>2. 개인정보의 수집범위</p> <ul style="list-style-type: none"> • 계정 등록시 수집하는 개인정보의 범위는 다음과 같습니다. <ul style="list-style-type: none"> ○ 필수항목 : 계정, 비밀번호, 비밀번호확인, 전자우편, 실명확인-여부, 휴대폰-서비스-이용시-이용, 주민등록번호-포함 ○ 선택항목 : 없음 	<p>2. 개인정보의 수집범위 및 수집방법</p> <p>① (생략)</p> <p>- 회사가 수집하는 개인정보의 범위</p> <ul style="list-style-type: none"> • 필수항목 : 계정, 비밀번호, 비밀번호확인, 전자우편 • 선택항목 : 없음
<p>6. 목적외 사용 및 제3자에 대한 제공 및 공유</p> <ul style="list-style-type: none"> • 귀하가 실명확인 여부가 필요한 회사 또는 제3자의 서비스를 사용하는 경우, 회사는 최소한의 범위에서 본 개인정보 취급방침에 따라 수집한 귀하의 개인정보를 일부 다른 아래와 같이 제공할 수 있습니다. <ul style="list-style-type: none"> ○ 제공 대상 정보 - 실명확인을 위한 이름, 주민등록번호 ○ 제공 대상 회사 - 한국신용평가정보㈜, 신용신용평가정보㈜ ○ 제공 정보의 이용목적 - 실명여부 확인에 필요한 회사 또는 제3자의 서비스 회원 가입시 입력하는 이름 및 주민등록번호와 관련하여 확인을 위한 목적으로 이용 ○ 제공 정보의 보유 및 이용기간 - 실명 여부 확인에 필요한 회사 또는 제3자의 서비스 가입시 	<p>6. 개인정보의 목적 외 사용 및 제3자에 대한 제공 및 공유</p> <p>① 회사는 본 개인정보취급방침에서 명시된 범위를 초과하여 이용하거나 타인 또는 타기업 기관에 귀하의 개인정보를 제공하지 않습니다. 다만, 귀하의 동의가 있거나 다음 각 호의 어느 하나에 해당하는 경우에는 예외로 합니다.</p> <ul style="list-style-type: none"> - 관계법령에 의하여 수사상의 목적으로 관계기관으로부터의 요구가 있을 경우 - 통계작성, 학술연구나 시장조사를 위하여 특정 개인을 식별할 수 없는 형태로 광고주, 협력사나 연구단체 등에 제공하는 경우 - 기타 관계법령에서 정한 절차에 따른 요청이 있는 경우

개인정보 수집 및 이용 목적 고지

※ 개인정보의 수집·이용 목적이 변경되었을 경우 변경사항 고지 필요

※ 고지 방법 : 이메일, 팩스, 전화 등

1-5. 만 14세 미만 아동의 정보 수집

법정 대리인의 동의 획득방법 예시

부모동의 이 학원동역 > 01 본인확인 > 03 부모동의 > 04 기본정보 입력 > 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 신용카드로 가입하실 수 있습니다. > 인증하기	부모 명의의 휴대폰으로 인증번호를 전송받아 가입하실 수 있습니다. > 인증하기	부모 범용 공인인증서로 가입하실 수 있습니다. (연리, 증권용 인증서 사용불가) > 인증하기
X 가입취소		

신용카드 인증
보호자(법정대리인)의 정보를 입력해 주세요.

보호자 이름	<input type="text"/>
주민등록번호	<input type="text"/> - <input type="text"/>
카드번호	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
유효기간	[01] 월 [2011] 년
비밀번호	<input type="text"/> XX
보호자 이메일	<input type="text"/> @ <input type="text"/>

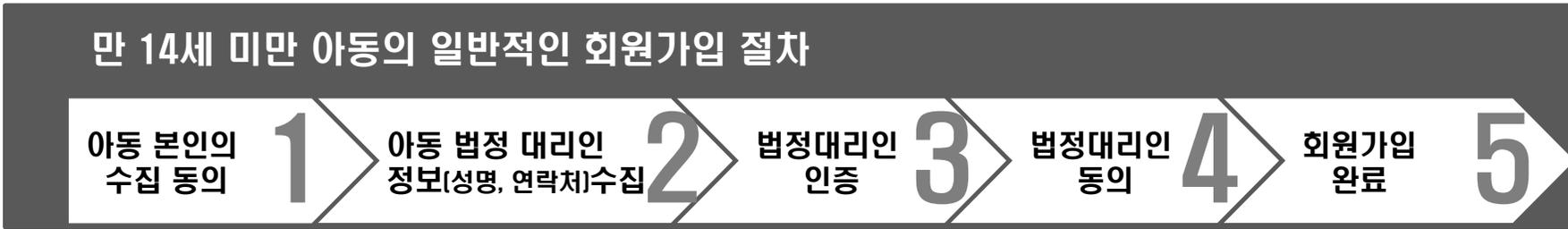
만 14세 미만 아동 동의

※ 만 14세 미만의 아동 개인정보를 처리하기 위한 법정대리인의 동의 필요

법정 대리인(보호자) 동의 인증

(ex : 신용카드, 휴대폰, 공인인증서 등)

법정 대리인의 정보 (성명, 연락처)



1-6. 최소정보 수집

민감정보 수집의 잘못된 사례

본인종교

가족종교

신장/체중/인상

병역

취미

최종학력

직업정보

직장정보

연소득(연봉)

본인재산

아버님정보

어머님정보

부모님재산

형제정보

현재거주상황

서비스 제공을 위해
필요한 최소한의 정보만 수집
**최소 정보에 대해 입증 책임
→ 개인정보처리자**

업종에 따라 최소정보
이외의 추가 정보수집 시
별도의 동의 획득 필요

정보주체의 미동의 시
그에 따른 불이익 고지

미동의 시에도 서비스 제공

1-7. 수집제한

✖ 민감정보 수집의 잘못된 사례

회원이 과거 성형했던 부위를 선택해주세요. - 필수 입력사항입니다.

<input type="checkbox"/> 눈성형	<input type="checkbox"/> 코성형	<input type="checkbox"/> 가슴성형	<input type="checkbox"/> 안면윤곽	<input type="checkbox"/> 지방흡입
<input type="checkbox"/> 지방이식	<input type="checkbox"/> 몸매성형	<input type="checkbox"/> 주름성형	<input type="checkbox"/> 브러성형(보톡스, 필러)	

다음

민감정보

- 원칙적 수집 금지
- 업무상 수집 필요 시 별도의 동의절차 필요

※ **민감정보 예시** : 사상, 신념, 정치적 견해, 성생활, 건강, 병력 (전염병, 성형 부위 등), 범죄경력 등

고유식별정보 수집 예시

실명인증

이름

주민등록번호 -

실명인증

아이핀(i-PIN) 인증

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

병원서비스(예약/조회/발급) 이용시, 인증이 필요합니다.

2009년 4월 1일 제정된 주민등록법 제37조(발칙) 제10호에 의한 타인의 정보 및 주민등록번호를 도용하여 사용하는 경우 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하게 됩니다.

아이핀(i-PIN)은 웹사이트에 주민등록번호 대신 이용할 수 있는 사이버 신원확인번호로서 인터넷 상에서 주민등록번호가 무단으로 유출되어 도용되는 부작용을 막기 위해 만들어진 서비스입니다.

고유식별정보

- 원칙적 수집 금지
- 고유식별정보 예시 : 정보주체 본인확인을 위한 주민등록번호, 여권번호, 운전면허번호 등
- 고유식별정보 수집 시 안전성 확보 조치 필요
- 안전성 확보 조치 예시 : DB 암호화, 문서 프로그램의 암호화 저장 (소규모 사업자의 경우 등)

1-8. 동의획득 시 구분

개인정보 수집 동의 시 구분 사례

000000 회원 이용약관

이름자가 제공자 하는 것이 "본점"이 아닌 본점의 갈라를 거쳐서 "본점" 업무를 수행한 후 당점이 물려하는 것으로 간주합니다. 본 당점이 말하는 이외의 이름자와 "본점"의 연회, 회주 및 책임사장이 겸하여는 대한민국에 법한 법인이 있습니다.

02. 제 2조 (정의)

위 000000 회원 이용약관에 동의합니다.

000000 서비스 이용약관

02. 제 2조 (용어 정의)

본 당점에서 사용하는 용어와 약칭은 다음과 같습니다.

① "서비스"라 함은 인터넷을 이용하여 제공하는 온라인 서비스로서 제공하는 내 송입의 전자 서비스 및 관련 제반 서비스를 의미합니다.

위 000000 서비스 이용약관에 동의합니다.

개인정보의 수집 및 이용목적

- 차별화 된 외부 정보 제공
- 맞춤형 맞춤 상품 제공
- 신규 서비스 개발의 개인 맞춤 서비스 제공을 위한 정보
- 상담 및 서비스를 위한 정보서비스 제공을 위한 정보 제공을 위한 정보서비스 제공

위 개인정보의 수집 및 이용목적에 동의합니다.

수집하는 개인정보의 항목 및 수집방법

본점을 회원 가입 시 서비스 이용을 위해 필요한 최소한의 개인정보를 수집합니다. 귀하가 본점의 서비스를 이용하기 위해서는 회원 가입 시 필수 수집 항목이 있으며, 의무사항이 아닌 경우 선택 항목은 선택하여 입력하셔도 서비스 이용에는 제한이 없습니다.

【필수 수집항목 시 수집항목】

위 수집하는 개인정보의 항목 및 수집방법에 동의합니다.

개인정보의 보유 및 이용기간

본점은 개인정보의 수집목적 또는 제공받은 목적이 달성된 때에는 귀하의 개인정보를 지체 없이 파기합니다.

개인정보 처리에 따른
동의 획득 시 각각의
동의사항을 구분하여
동의를 받아야 한다

- 수집 및 이용 동의 항목
- 제3자 제공
- 목적 외 이용 · 제공
- 자사회원을 대상으로 재화나 서비스 홍보 및 판매 권유 목적

1-10. 업무위탁과 제3자 제공 비교



	업무위탁	제3자 제공
정의	개인정보처리자의 사업목적을 달성하기 위해 수탁자에게 개인정보를 제공하는 경우	개인정보처리자 외의 제3자의 이익이나 사업목적 달성을 위해 제3자에게 개인정보를 제공하는 경우
의무내용	<ul style="list-style-type: none"> 고지임무 : 직접 마케팅 업무위탁으로 인한 개인정보 제공 시 공개임무 : 위탁 사실(위탁내용, 수탁자) 공개 	<ul style="list-style-type: none"> 고지임무 : 제3자 제공에 대한 고지 동의임무 : 제3자 제공에 대한 정보주체 동의 획득 <p><small>* 동의항목(4가지): 제공받는 자, 개인정보 항목, 목적, 보유 및 이용기간</small></p>
예시	<ul style="list-style-type: none"> 계약체결 대행 서비스(텔레마케팅 등) 관리 대행 서비스(상품배송, AS 등) 전산관리 위탁 서비스(시스템, DB 개발 등) 	<ul style="list-style-type: none"> 금융서비스 제공을 위한 이메일 홍보 보험상품 소개를 위한 텔레마케팅 등

1-10. 업무위탁과 제3자 제공 비교

개인정보 위탁



개인정보
제3자 제공

의미

- 업무 아웃소싱

- 제휴, 공동상품 판매
- 기업간 업무 협약

전제조건

- 개인정보 처리 업무위탁 시 문서로 명시
 - 위탁업무의 수행 목적 외 개인정보의 처리금지
 - 개인정보의 관리적·기술적 보호조치
- 업무위탁 시 정보주체가 쉽게 확인 가능

- 정보주체의 동의 필요항목
 - 제공받는 자
 - 제공받는 자의 개인정보 이용목적
 - 제공하는 개인정보 항목
 - 제공하는 자의 개인정보 보유 및 이용기간
- 동의거부 시 불이익 사실 고지 의무
- 미동의 시에도 서비스 제공
- 목적 외 이용 및 제공 금지

유의사항

- 위탁 사실에 대한 고지 (동의획득 불필요)

- 수집 목적 외 이용 및 제3자 제공 금지
- 제공 사항에 대한 별도 동의 획득
- 미동의 시에도 서비스 이용 허용 (미동의 시 불이익 내용 고지)

1-11. 업무위탁 시 공개내용

위탁에 대한 올바른 공개 예시

****전자 패밀리 서비스 이행을 위해 개인정보 취급 업무 중 일부를 아래와 같이 외부 전문 업체에 위탁하여 운영하고 있습니다.**

위탁업체	위탁업무 내용
AAA	회원제 서비스 이용에 따른 본인 실명 확인
BBB	온라인 광고, 캠페인 집행을 위한 위탁- 광고, 이벤트 등과 같은 마케팅 업무 수행에 필요한 고객 정보 추출, 활용
CCC	마케팅 업무 운영 대행을 위한 위탁- 이벤트 당첨자 상품 배송을 위한 고객정보 추출, 제품/기업 및 이벤트 홍보 메일전송을 위한 고객정보추출등과 같은 마케팅 업무 운영
DDD	고객응대 업무 효율성 제고를 위한 위탁 - **전자 패밀리 회원 고객문의 응대, 물품 구매관련 및 배송관련 고객문의응대, 만족도 조사(제품구매,배송설치,서비스)
EEE	제품 구매에 따른 물품 배송 및 제품설치

개인정보 처리 업무위탁 시 공개내용

- 위탁업무의 수행 목적 외 개인정보의 처리금지
- 개인정보의 관리적·기술적 보호조치 관리감독

개인정보 처리 업무 위탁 시 수탁자 및 해당 내용 공개

1-13. 제3자 제공 고지와 동의

제3자 제공 고지 및 동의 예시

약관 동의

- OO통합회원 약관

제1조 (목적)

[필수] 통합 회원 이용 약관에 동의합니다.

- 0000 이용약관

제 1 장 총칙

[필수] 0000 이용약관에 동의합니다.

- 개인정보 수집, 이용 (필수)
 - 1. 개인정보 수집, 이용
- 고객 편의제공을 위한 취급위탁(선택)
 - 2. 고객 편의제공을 위한 취급위탁

[필수] 개인정보 수집, 이용에 대해 동의합니다. [선택] 고객편의 제공을 위한 취급위탁에 대해 동의합니다.

- 결합 및 제휴서비스를 위한 동의(선택)
 - 3. 결합,제휴서비스를 위한 동의

보이는 귀사가 서비스 제공(이용목적)을 위해 제공받는 자에게 해당 정보를 제공함에 동의합니다.

[선택] 결합, 제휴서비스를 위한 정보제공에 동의합니다.

점검사항

제3자 제공 시 고지해야 할 사항

1. 개인정보를 제공받는 자
2. 제공받는 자의 이용 목적
3. 제공하는 개인정보 항목
4. 제공받는 자의 보유 및 이용기간
5. 개인정보 수집 출처

반드시 별도 동의 필요

개인정보 제공 미동의 시
서비스 이용이
가능하도록 해야 한다

1-14. 제3자 제공 예시

제3자 제공 시 올바른 예시

이용약관

[전자레탈리] 이용약관

제 1 조 (목적)

이 약관은 전자 주식회사(이하 "전자"라 합니다)가 운영하는 전자 대표사이트, "닷컴, B2B, 모바일닷컴, 디지털프라자, 쿠팡, 파워리넷과 전자서비스

위의 개인정보 수집 및 이용에 대한 내용에 동의하십니까?

동의

동의안함

홈페이지/ 닷컴 회원가입

[정보제공]

홈페이지/ 닷컴 동시가입에 동의하실 경우 본 사이트 회원가입을 통해 입력하신 정보 중 회원 ID, 이름, 생년월일, 성명, 이메일주소, 주소, 연락처, 직업, 내/외국인 여부 및 미성년자의 경우 법정대리인의 이름, 연락처, 메일주소를 홈페이지/ 닷컴(주) 운영에 제공합니다.

위의 정보제공 내용에 동의하십니까?

동의

동의안함

[메일수신]

홈페이지/ 닷컴 동시가입에 동의하실 경우 홈페이지/ 닷컴에서 발송하는 정보 메일을 수신하시게 됩니다. 메일 수신을 원치 않을 경우, 홈페이지/ 닷컴의 개인정보수정을 통해 수신 거부 설정을 하실 수 있습니다.

위의 메일수신 내용에 동의하십니까?

동의

동의안함

제3자 제공 시 잘못된 예시

가입여부 및 실명인증 확인

기존에 회원가입이 되신 분은 실명인증시 가입 여부를 함께 확인하실 수 있습니다.

이름:

주민번호: -

이용약관

제 1 조 (목적 등)

1) 이 약관(이하 "이 약관"이라 합니다)은 이하 "회사"라 합니다.)가 운영하는 인터넷 사이트 (www. .co.kr 및 동 사이트의 기본 DB를 공유하는 모든 사이트를 말함. 이하 " "라 합니다)에서 제공하는 제반 서비스(이하 "서비스"라 합니다)를 이용자가 이용할 때 이 약관과 관련하여 회원의 권리와 의무 및 책임사항을 규정함을 목적으로 합니다.

온라인 회원 이용약관에 동의

개인정보 취급방침

개인정보 취급방침

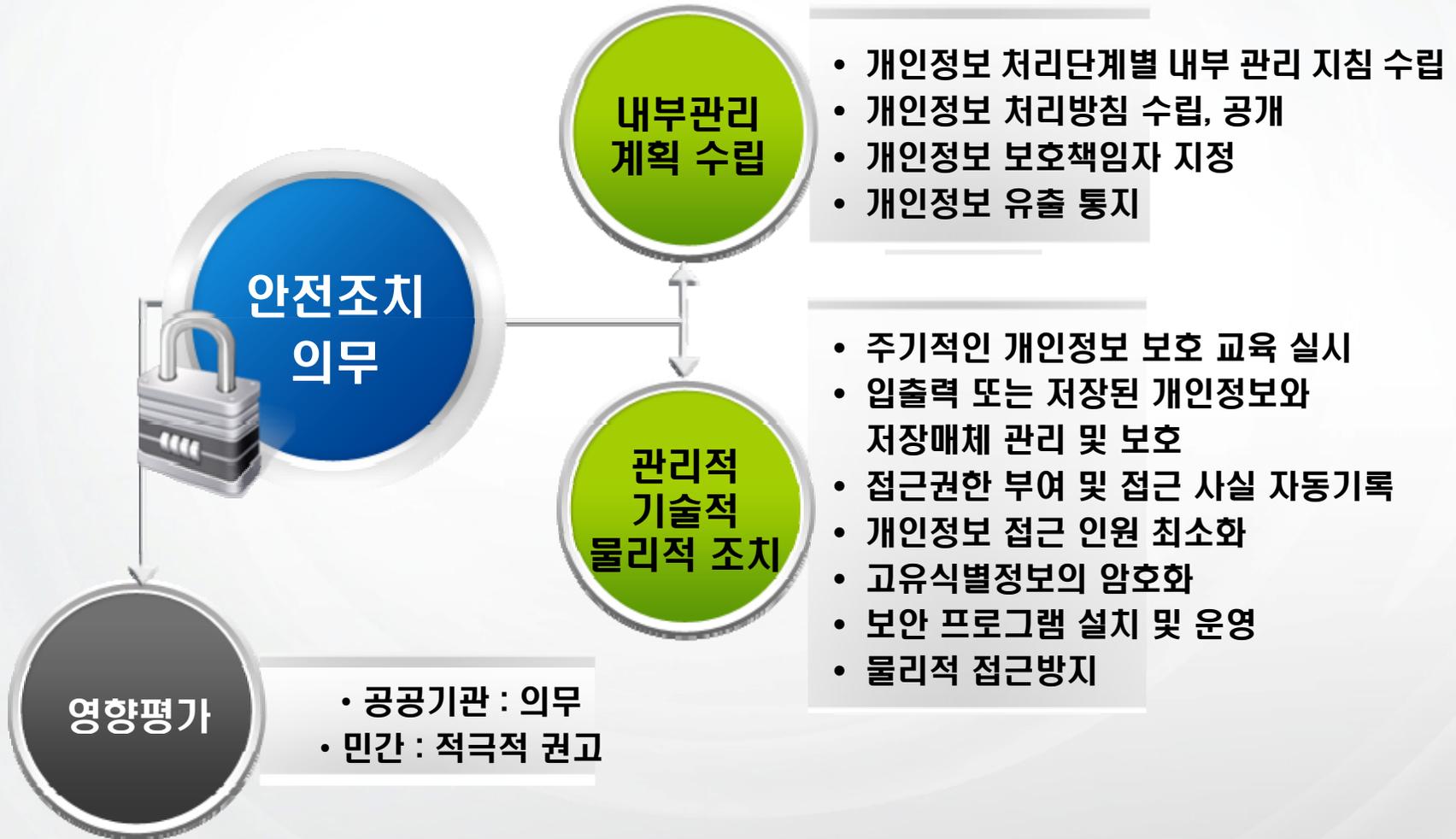
개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함)을 말합니다.

(주) 는 회원의 개인정보보호를 매우 중요시하며, 정보통신망이용촉진등에 관한

개인정보 취급방침에 동의

1-15. 안전관리 주요 점검사항

{ 점검사항 }



- 개인정보 처리단계별 내부 관리 지침 수립
- 개인정보 처리방침 수립, 공개
- 개인정보 보호책임자 지정
- 개인정보 유출 통지

- 주기적인 개인정보 보호 교육 실시
- 입출력 또는 저장된 개인정보와 저장매체 관리 및 보호
- 접근권한 부여 및 접근 사실 자동기록
- 개인정보 접근 인원 최소화
- 고유식별정보의 암호화
- 보안 프로그램 설치 및 운영
- 물리적 접근방지

영향평가

- 공공기관 : 의무
- 민간 : 적극적 권고

1-16. 개인정보보호 조직 구성

중·대기업 예제



소기업 예제



1-17. 내부관리계획 수립 및 적용

내부관리계획 목차 예시

개인정보보호 내부관리 계획

[목차]

제1장 총칙

- 제1조(목적)
- 제2조(적용범위)
- 제3조(용어의정)

제2장 개인정보보호 의무와 책임

- 제4조(개인정보관리 책임자)
- 제5조(개인정보취급자)

제3장 개인정보 관리 절차

- 제6조(개인정보보호 준수사항)
- 제7조(접근통제)
- 제8조(접속 기록의 위변조 방지)
- 제9조(개인정보의 암호화)
- 제10조(개인정보 관리에 대한 감독 및 고충처리)
- 제11조(개인정보취급업무의 위탁)
- 제12조(개인정보의 누설금지)

제4장 개인정보보호 교육

- 제12조(개인정보보호 교육 계획의 수립)
- 제13조(개인정보보호 교육의 실시)

제5장 내부관리계획의 승인 및 검토

- 제14조(내부관리계획의 타당성 검토 및 승인)
- 제15조(내부관리계획의 공표)
- 제16조(별첨 및 공지)

내부관리계획
승인
(CEO, CPO 등)

사내 배포

개선계획 수립
(연간 1회)

적용 및
자체 감사

1-18. 개인정보 처리방침 작성

개인정보 처리방침 공개

■ 개인정보 처리방침

개인정보보호를 위해 어떠한 조치가 취해지고 있는지 알려드립니다.

- | | | |
|---------------------|-----------------------------|-----------------|
| 01. 총칙 | 08. 개인정보제공 | 15. 링크사이트 |
| 02. 개인정보의 수집범위 | 09. 수집한 개인정보의 위탁 | 16. 게시물 |
| 03. 개인정보 수집에 대한 동의 | 10. 이용자 및 법정대리인의 권리와 그 행사방법 | 17. 이용자의 권리와 의무 |
| 04. 수집하는 개인정보 항목 | 11. 루기에 의한 개인정보 수집 | 18. 광고성 정보 전송 |
| 05. 개인정보의 수집 및 이용목적 | 12. 개인정보에 관한 민원서비스 | 19. 고지의 의무 |
| 06. 개인정보의 보유 및 이용기간 | 13. 의견수렴 및 불만처리 | |
| 07. 개인정보의 파기절차 및 방법 | 14. 개인정보보호를 위한 기술 및 관리적 대책 | |

01. 총칙

- ① 개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 식별할 수 있는 것을 포함합니다)를 말합니다.
- ② 당사는 귀하의 개인정보보호를 매우 중요시 여기며, *정보통신망 이용촉진 및 정보보호에 관한 법률 상의 개인정보보호 규정 및 정보통신부가 제정한 *개인정보처리방침을 통하여 귀하에게 제공하는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며 개인정보보호를 위해 어떠한 조치가 취해지고 있는지 알려드립니다.

정보주체를 위한 내용별
바로가기 버튼 설정

포함내용

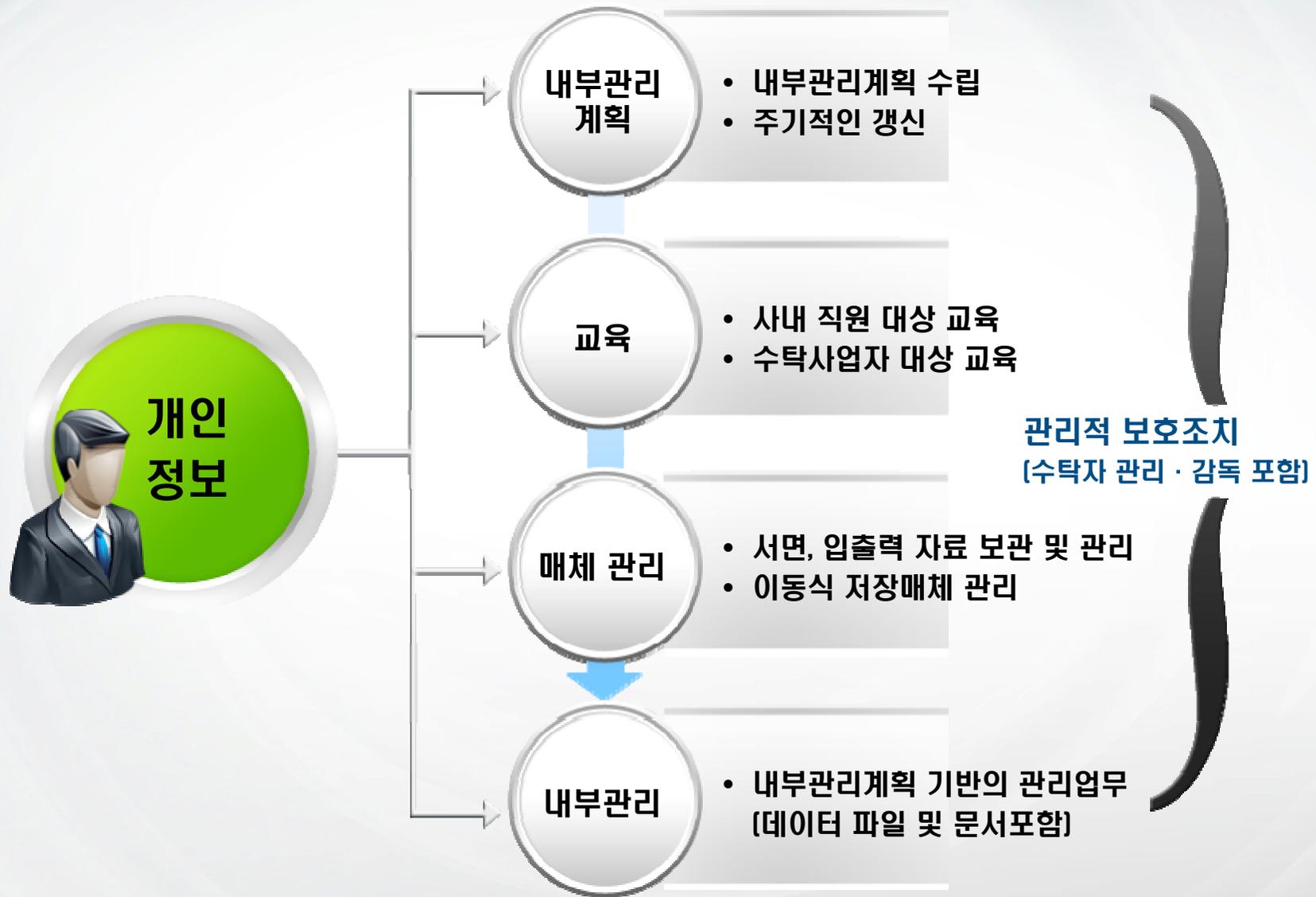
- 개인정보의 처리 목적
- 개인정보의 처리 및 보유기간
- 개인정보의 제3자 제공에 관한 사항(해당되는 경우)
- 개인정보의 위탁에 관한 사항(해당되는 경우)
- 정보주체의 권리 의무 및 그 행사 방법

공개방법

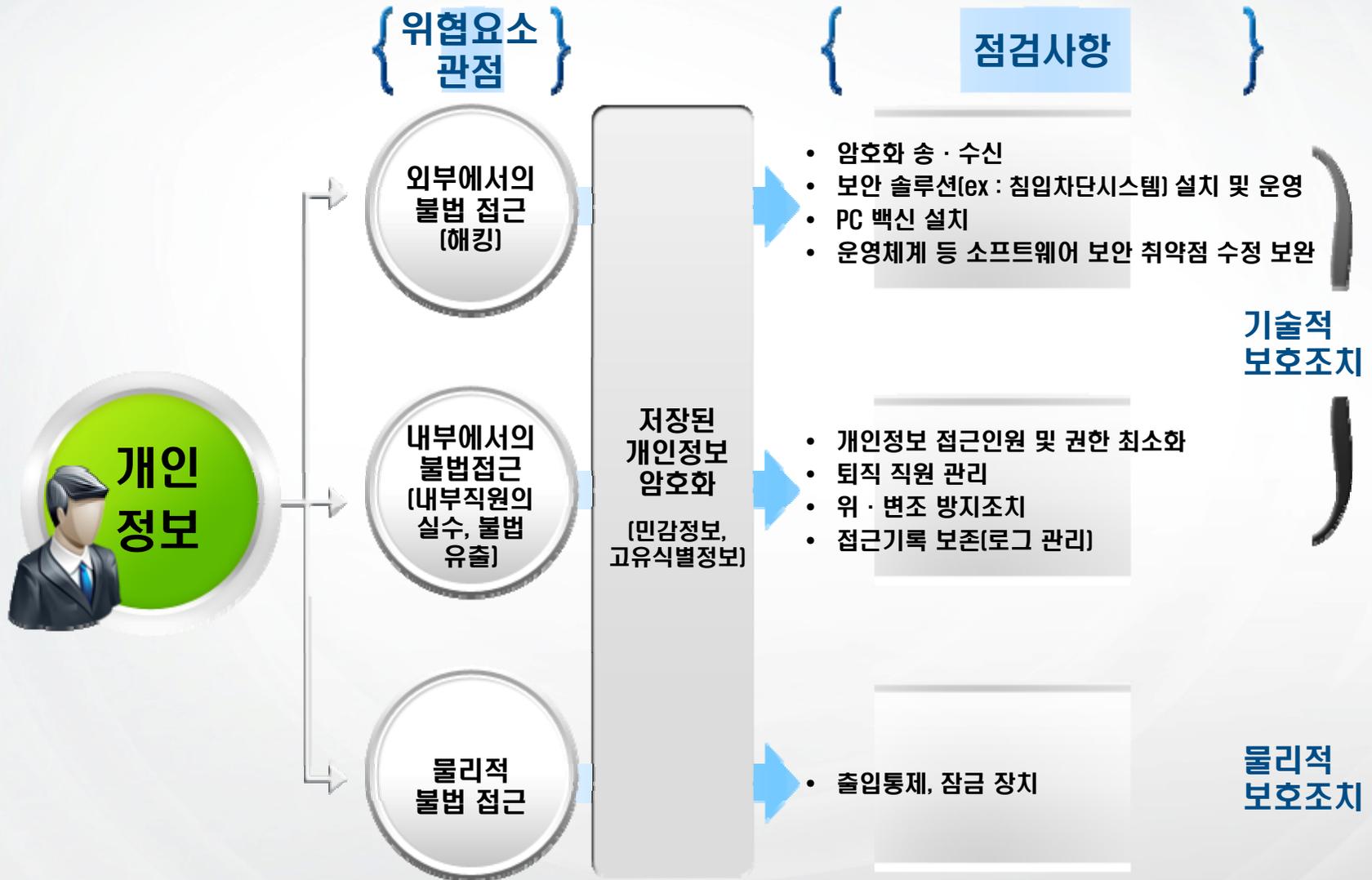
- 홈페이지 첫 화면 게재
- 종이문서의 경우 이용약관서 등에 명기
- 관보게재(공공기관)

※ 개인정보 처리방침은 정보주체가 쉽게 확인할 수 있도록 공개해야 하며, 변경사항 발생 시 별도고지

1-19. 관리적 보호조치



1-20. 기술적 · 물리적 보호조치



1-21. 파기시점과 방법

개인정보 파기



{ 파기 시점 }

- 개인정보의 처리목적 달성 등
- 개인정보가 불필요해진 경우

<예시>

- 회원 탈퇴
- 계약 또는 이벤트 종료
- 이용자의 요구

{ 파기 방법 }

- 복구 또는 재생이 불가능하도록 파기

<예시>

- 종이 : 세단기 분쇄 또는 소각
- 데이터 : 소거 S/W 사용

※ 타 법령 등에 의거하여 개인정보의 보존이 필요할 경우
다른 개인정보와 분리 저장 관리

1-22. 열람, 정정 및 삭제, 처리정지

개인정보 열람 권리



의미

- 정보주체의 열람요구
 - 개인정보의 항목 및 내용
 - 개인정보의 제3자 제공현황
 - 개인정보 처리에 대한 동의현황

유의사항

- 열람제한 거부에 대한 사유발생 시 정보주체에게 통보

개인정보 정정, 삭제 권리



- 개인정보를 열람한 정보주체가 정정 및 삭제 요구 (단, 다른 법령에 수집대상이 될 경우 삭제 요구 불가능)

- 정정, 삭제 결과에 대한 통보
- 정정, 삭제 요구사항의 확인 위한 증거자료 제출

개인정보 처리정지 권리

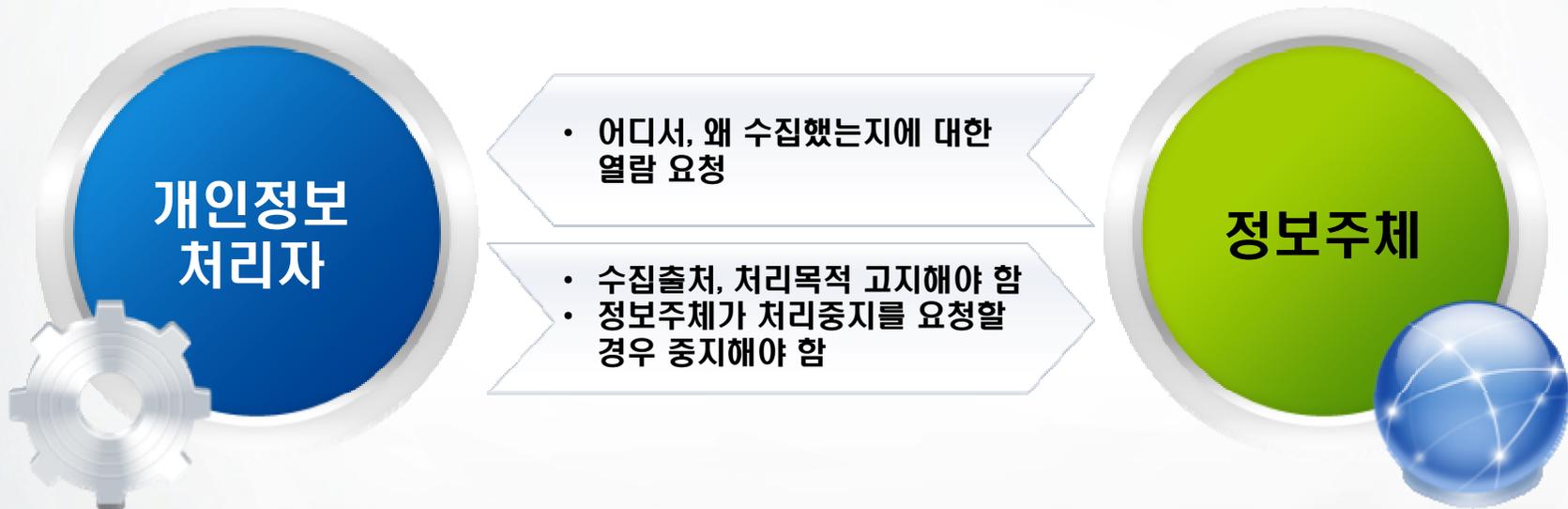


- 정보주체의 처리정지 요청

- 처리정지 거부에 대한 사유발생 시 정보주체에게 통보

1-23. 수집 출처 고지

정보주체 이외로부터 개인정보를 수집한 경우



※ 예외조항 : 국가안전, 외교상의 비밀, 범죄의 수사, 조세 관련 등 고지로 인해 생명, 신체를 해할 우려가 있을 경우나 재산과 그 밖의 이익을 부당하게 침해할 경우,

1-24. 제3자 양도

사업의 영업 양수 등에 따른
개인정보 이전 통지

영업의 양도 및 합병 등으로 인해
개인정보 이전 시 해야 할 사항

인수합병에 따른 제3자 양도 이전 통지예제

1. 주식회사

간의 합병안내

주식회사 주식회사 및 주식회사 은 경영효율성을 증대시키고 유·무선 통신사업의 결합을 통한 시너지효과를 극대화함으로써 국내외 경영환경 변화에 적극 대처하여 세계적인 경쟁력을 보유한 통신회사로 성장하기 위하여 2010. 1. 1. 자 합병을 결정하였습니다. 은 합병 후에도 계속하여 고객이 원하는 융합형 서비스를 실현하고 고객의 편익을 제공하는 등 국가경제 발전에 기여할 것입니다.(단, 본 합병은 방송통신위원회의 합병인가심사결과 등 합병절차의 결과에 따라서 성사되지 않을 수도 있습니다.)

합병법인인 주식회사 의 개요는 다음과 같습니다.

- 대표이:
- 주 소 :
- 전화번
- 임직원수 : 2380명
- 주요사업 : 이동통신서비스(음성전화, 무선데이터, 부가통신서비스 등)
- 연 혁 : 설립(1996. 7.), 개인휴대통신서비스(PCS) 서비스 개시(1997. 10).

주식회사 은 합병등기가 이루어지는 날부터 주식회사 의 관리 의무를 포괄적으로 승계하여, 주식회사 을 대신하여 고객님에게 서비스를 제공하게 됩니다. 합병완료 시 주식회사 이 제공하는 서비스는 요금, 할인제도 등을 포함하여 주식회사 품이 합병 전에 제공한 것과 동일한 내용이 될 것입니다. 다만, 고객님은 주식회사 과 체결한 서비스 이용계약 및 이용약관의 조건에 따라 서비스 이용계약을 해지할 수 있습니다.(단, 기간을 약정하여 서비스 이용계약을 체결하신 고객님이 이용계약을 해지하시는 등의 경우 계약 규정에 따라 위약금이 부과될 수 있습니다.)

주식회사 의 서비스이용계약해지절차는 다음과 같습니다.
※ 전화서비스 이용약관 제26조, 인터넷전화070 이용약관 제22조, 시내전화서비스 이용약관 제20조 등 [계약의 해제, 해지] 이용자가 계약을 서비스 개를 전에 해제하거나 개를 후에 해지하려는 경우 그 뜻에 통지하여야 합니다.

합병에 따른 서비스 이용계약에 관한 문장은 고객센터() 로 연락주시거나 홈페이지()의 이용약관을 참조하시기 바랍니다.

개인정보 이전 통지 및 합병안내 Q & A

Q 1. 유무선 통합을 통하여, 고객님께 보다 나은 서비스를 제공해 드리기 위하여, 2010년 1월 1일자로 으로 합병하게 되었습니다. 이와 관련하여, 기존 서비스를 이용하시던 고객님께 고객님의 정보가 으로 이전한다는 내용을 안내드리기 위해서 안내문을 발송해드린 것입니다. 합병 이후에도 고객님의 서비스는 기존과 동일하게 제공되며, 앞으로 다 좋은 서비스 제공을 위하여 노력하겠습니다. 그리고 합병안내 및 개인정보이전 통지는 정보통신법 및 합병관련 법률위 고시에 따른 법적인 준수사항입니다. 이해 바랍니다. 감사합니다.

Q 2. 합병을 한다는데 그항 A/S는 어떻게 되는 건가요?

A 걱정하지 않으셔도 됩니다. 회사가 여러워서 합병을 하는 것이 아니라 고객님들께 다 좋은 서비스를 제공해 드리기 위하여 합병하는 것이어서 현재 받고 계신 서비스는 그대로 유지/유지됩니다. 또한 이 제공했던 서비스 요금, 할인제도 등을 포함하여 합병 전에 제공한 것과 동일하게 제공되나 고객님은 안심하시고 이용하셔도 됩니다. 감사합니다.

Q 3. 기존 회사가 망하거나 없어지는 건가요?

A 아닙니다. 회사가 여러워서 합병을 하는 것이 아니라 고객님들께 다 좋은 서비스를 제공해 드리기 위하여 합병하는 것이어서 이 제공했던 서비스는 동일하게 을 통하여 제공되며, 유선과 무선을 통합하여 다 나은 서비스를 제공해 드릴 예정입니다. 감사합니다.

Q 4. 개인정보가 다른 회사로 이전한다는 건 개인정보 유출이런가요?

A 기존통신 사업자의 합병은 정보기관의 검토 및 승인을 거쳐 합병을 하게 되며, 이용자보호 및 개인정보 유출 및 오남용 문제가 없도록 관련 법규를 준수하고 있습니다. 또한 고객님의 지속적인 서비스 제공을 위하여 합병 법인인 으로의 개인정보 이전은 필수적입니다. 그리고 합병 이후에도 고객님의 개인정보는 철저한 보호조치를 사용할 것입니다. 감사합니다.

Q 5. 내 개인정보는 어떻게 되는 건가요?

A 합병 후, 에서 고객님께 동일한 서비스를 제공해야 하기 때문에 이전된 개인정보는 합병 법인인 이 관리하게 됩니다. 제 준수하는 것으로 개인정보를 안전하게 보관을 하는 것이 아니라 통합 법인 운영에 따른 관리법인의 변경으로 이해하시면 됩니다. 고객님의 개인정보는 지금보다 더 안전하게 관리하게 예정입니다. 감사합니다.

1-25. 집단분쟁 및 단체소송

집단분쟁

단체소송

목적

- 유사 유형으로 다수 정보주체에게 침해발생시 일괄적 분쟁조정
- 개인정보 분쟁조정 결과의 구속력

- 다수의 정보주체가 소송제기가 불가능한 경우, 일정한 자격을 갖춘 단체가 소송 제기

신청권자

- 국가, 지방자치단체, 개인정보 보호단체, 개인정보처리자 등
- 단, 정보주체가 직접 신청할 수 없다

- 소비자 단체와 비영리 민간단체

신청대상 사건

- 정보주체의 피해 또는 권리침해가 다수에게 같거나 비슷한 유형

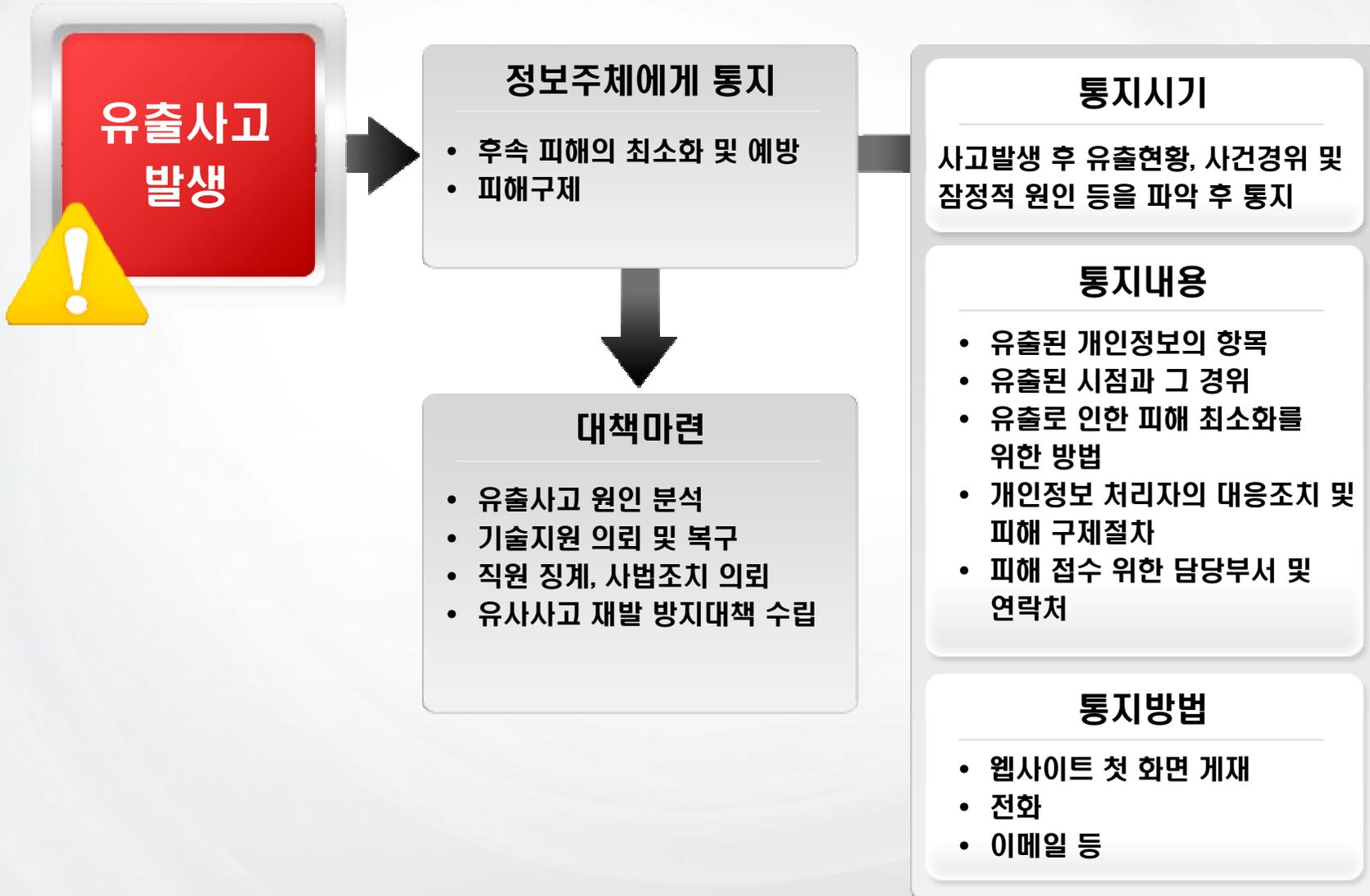
- 분쟁조정위원회의 조정을 거부하거나 조정결과를 수락하지 아니한 경우
- 단체소송 전 집단분쟁조정제도 이행

효력

- 분쟁 조정결과 → 결과수락 → 위원회 권고

- 민사소송법 적용

1-26. 개인정보 유출 통지



1-27. 개인정보 관련 처벌 규정

개인정보보호법 처벌 규정

구분	주요내용	처벌 및 벌칙	구분	주요내용	처벌 및 벌칙	구분	주요내용	처벌 및 벌칙	
수집·이용	정보주체의 동의없는 개인정보 제3자 제공(17조)	5년 이하 징역 또는 5천만원 이하 벌금	제3자·위탁	동의없는 개인정보 제3자 제공(17조)	처벌 및 벌칙 5년 이하징역 또는 5천만원 이하 벌금	정보주체 권익보호	개인정보의 정정·삭제요청에 대한필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제3자에게 제공한 자(제36조)	2년 이하 징역 또는 1천만원 이하 벌금	
	개인정보의 목적외 이용·제공(18조, 제19조, 제26조)			직접마케팅 업무위탁으로 인한 개인정보 제공 시 정보주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18, 제26조)	3천만원 이하 과태료		개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자(제37조)		
	민감정보 처리기준 위반(제23조)			업무위탁시 공개의무 위반(제26조)	1천만원 이하 과태료		개인정보 유출사실 미통지(제34조)	3천만원 이하 과태료	
	고유식별정보 처리기준 위반(제24조)			개인정보의 누설 또는 타인 이용에 제공(제59조)	5년 이하 징역 또는 5천만원 이하 벌금		정보주체의 열람 요구의 부당한 제한·거절(제35조)		
	부정한 수단이나 방법에 의해 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한 자(제59조)	3년 이하 징역 또는 3천만원 이하 벌금	개인정보의 훼손, 멸실, 변경, 위조, 유출(제59조)	영상정보처리기기 설치목적과 다른 목적으로 임의 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자(제25조)	3년 이하 징역 또는 3천만원 이하 벌금		정보주체의 정정삭제요구에 따라 필요 조치를 취하지 아니한 자(제36조)		
	개인정보의 수집기준 위반(제15조)	5천만원 이하 과태료	개인정보 아전반전	직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자(제60조)	2년 이하 징역 또는 1천만원 이하 벌금		처리정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자(제37조)	1천만원 이하 과태료	
	만 14세 미만 아동의 개인정보 수집시 법정대리인 동의획득의무 위반(제22조)			안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자(제24조, 제25조, 제29조 위반)	3천만원 이하 과태료		시정명령 불이행(제64조)		
	탈의실·목욕실 등 영상정보처리기기 설치 금지 위반(제25조)			영상정보처리기기 설치·운영기준 위반(제25조)	3천만원 이하 과태료		정보주체의 열람, 정정·삭제, 처리정지 요구 거부시 통지의무 불이행(제35조, 제36조, 제37조)		
	직접마케팅 업무위탁으로 인한 개인정보 제공 시 정보주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18, 제26조)	개인정보를 분리해서 저장·관리하지 아니한 자(제21조)		1천만원 이하 과태료	관계물품·서류 등의 미제출 또는 허위제출(제63조)				
	최소한의 개인정보 외 정보의 미동의를 이유로 재화 또는 서비스 제공을 거부한 자(제16조, 제22조)	개인정보처리방침 미공개(제30조)			3천만원 이하 과태료		출입·검사를 거부·방해 또는 기피한 자(제63조)		
주민등록번호를 제공하지 아니할 수 있는 방법 미제공(제21조)	개인정보관리책임자 미지정(제31조)	파기				개인정보 미파기(제21조)	3천만원 이하 과태료		
동의획득방법 위반하여 동의받은 자(제22조)	1천만원 이하 과태료			영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)					

2-1. 개인정보 관리적 · 기술적 보호조치

개인정보의 보호조치

관리적 보호조치

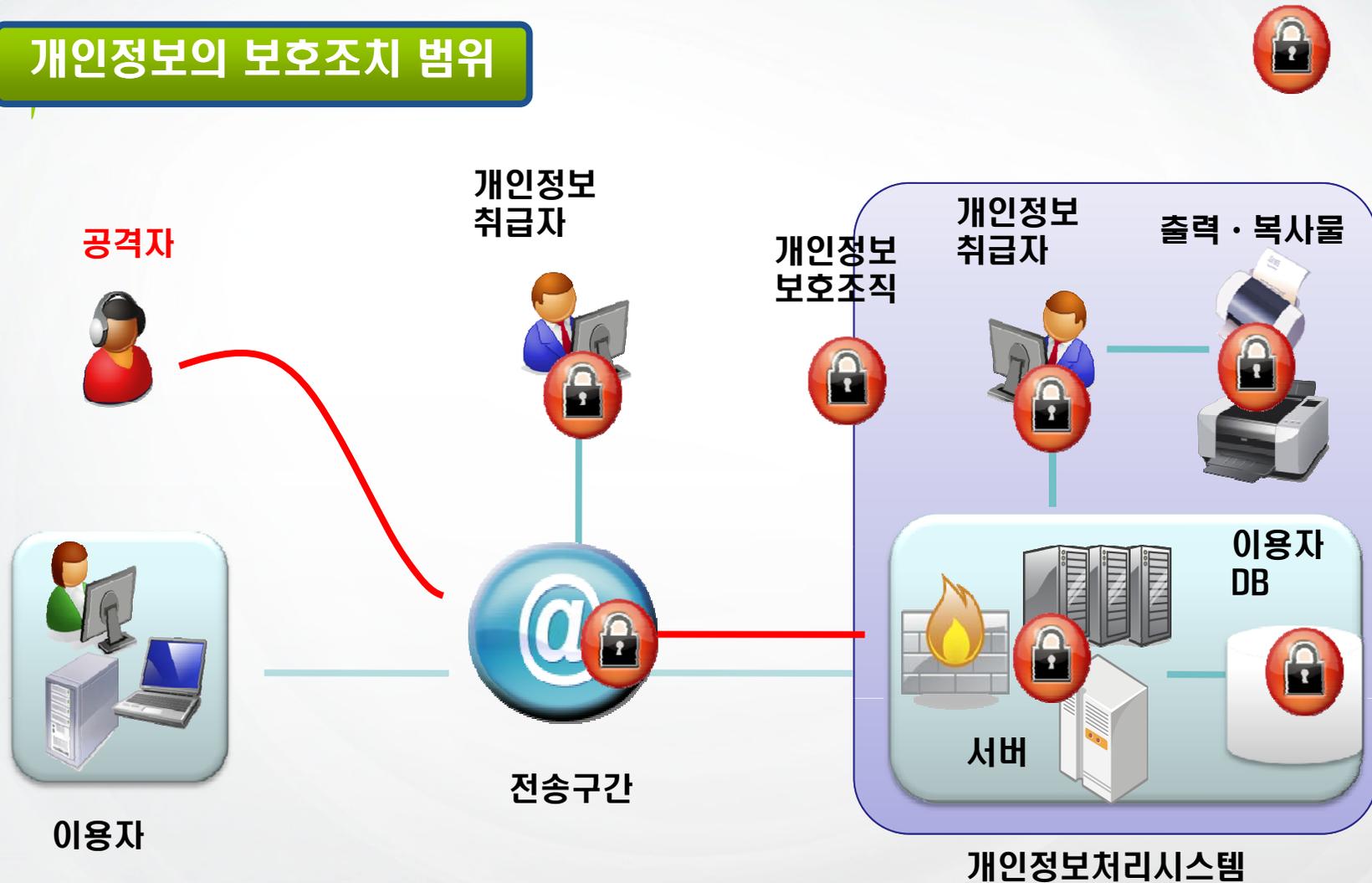
- 내부관리계획수립
- 개인정보 보호조직 구성
- 개인정보 취급자 교육
- 관리적 · 물리적 접근통제
- 출력 · 복사 시 보호조치
- 개인정보 표시제한

기술적 보호조치

- 개인정보 처리시스템의 관리
- 기술적 접근통제
- 접속기록의 위 · 변조 방지
- 개인정보 암호화
- 보안서버구축
- 악성프로그램 방지
- 개인정보 파일/문서 통제
- 개인정보 파기

2-2. 개인정보 관리적 보호조치

개인정보의 보호조치 범위



2-2. 개인정보 관리적 보호조치

내부관리계획 수립

개인정보보호 활동이 임기응변식이 아닌 체계적이고 전사적인 계획하에 수행될 수 있도록 내부관리계획을 수립·시행

공공기관

공공기관이 처리하는 개인정보의 안전한 보호관리를 위해 필요한 자체 개인정보계획 수립 또는 규정을 제정하여 시행한다.

민간기업

개인정보가 분실·도난·누출·변조 또는 훼손되지 않도록 안전성을 확보하기 위하여 내부관리계획을 수립하고, 최고 경영층의 승인을 받아 시행한다

2-2. 개인정보 관리적 보호조치

내부관리계획 주요내용

개인정보 보호조직

- 개인정보관리책임자(CPO) 지정
- 개인정보취급자 지정
- 담당자별 업무 및 임무 지정

개인정보 취급자 교육

- 교육계획 수립 및 정기적인 교육 실시

보호조치 세부사항

- 접속기록 위·변조 방지
- 개인정보의 암호화(주민번호, 계좌번호 등 금융정보)
- 악성프로그램 침투방지
- 출력·복사시 보호조치
- 개인정보 출력 표시 제한

기타

- 보안서약서 작성, 임직원 인식제고
- 개인정보 노출 방지 대책 등

2-2. 개인정보 관리적 보호조치

개인정보보호 조직의 구성

조직특성에 적합한 개인정보보호 조직을 구성하고, 구성원 각자의 책임과 권한을 명백히 규정하여 효율적이고 책임있는 개인정보보호 업무 수행

<해야 할 일>

담당자 지정

- 공공기관 : 개인정보관리책임자, 담당자, 개인정보취급자
- 민간기업 : 개인정보관리책임자, 개인정보보호취급자

안내

- 공공기관 : 개인정보관리책임자 안내
- 민간기업 : 개인정보관리책임자 안내

2-2. 개인정보 관리적 보호조치

개인정보관리책임자 역할

공공기관

- 1) 개인정보보호 계획 및 방침 수립/시행
- 2) 개인정보침해 관련 민원의 접수/처리
- 3) 개인정보 처리상태의 점검 및 감독
- 4) 각종 개인정보보호관련 통계 및 자료 취합
- 5) 소속된 다른 공공기관의 개인정보보호 관련 업무 총괄
- 6) 그밖에 개인정보보호교육 등 그 기관의 개인정보보호를 위해 필요한 업무

민간기업

- 1) 개인정보보호조직 구성·운영의 총괄
- 2) 내부관리계획의 수립 및 승인
- 3) 개인정보의 기술적·관리적 보호조치 기준 이행 총괄
- 4) 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검
- 5) 이용자의 개인정보에 관한 고충이나 의견의 처리 감독
- 6) 임직원, 개인정보취급자 및 수탁자, 대리점 등에 대한 교육 등 인식제고
- 7) 그 밖에 이용자의 개인정보보호에 필요한 사항

2-2. 개인정보 관리적 보호조치

개인정보 취급자의 범위

일반적으로 업무수행에 있어서 개인정보를 처리하는 담당자는 모두 개인정보 취급자의 범위에 포함

공공기관

정보주체의 개인정보에 대한 접근권한을 가진 자로서 공공기관에서 수집하여 보유하고 있는 개인정보를 취급하는 자로서 웹사이트 관리자, CCTV 관리자, 열람 및 정정·삭제 업무 담당자 등 업무수행에 있어 개인정보를 취급하는 담당자는 모두 개인정보취급자의 범위에 포함

민간기업

정보통신서비스 제공자의 사업장 내에서 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자로서 시스템 운영자와 정보보호 담당자 등이 업무수행을 위해 개인정보를 취급할 경우 개인정보 취급자에 포함

※ 개인정보취급자 최소제한 원칙 : 개인정보보호법 제16조(개인정보의 수집 제한)

2-2. 개인정보 관리적 보호조치

개인정보보호교육

- 개인정보보호정책의 실효성 확보를 위해 개인정보취급자의 인식을 제고시키고 전문성 향상을 위한 교육 필요

교육대상

- 개인정보취급자(위탁 받은 자 및 대리점 등 포함)
* 개인정보 처리자 : 공공기관, 법인, 단체 및 개인 등

교육내용

- 개인정보보호 기초지식, 침해 및 위반 사례, 개인정보보호 우수사례, 개인정보관리방법, 권익보호 및 침해 등을 교육

교육방법

- 집합, 사이버 교육, 워크샵 등 다양한 교육방식을 기관의 특성과 내용에 따라 자유롭게 선택하여 교육

교육주기

- 정보통신서비스제공자의 경우 연 2회 이상 실시(의무) * 정보통신망법
• 개인정보보호법 : 정기적인 교육 실시 (28조)

2-2. 개인정보 관리적 보호조치

개인정보 실태 관리

개인정보의 수집·활용이 다양화, 전문화, 체계화 됨에 따라 각 기관의 개인정보 관리체계에 대한 정례화·체계화 된 실태관리를 통하여 각 기관의 관련 법규 준수 및 이행여부 점검

공공 기관

년 2회 이상 점검관리(내부적으로도 실태조사 가능)

민간 기업

- 개인정보 처리방침, 보안서버 등 온라인 조사
- 자료제출 요구 또는 사업장에 출입하여 검사

2-2. 개인정보 관리적 보호조치

관리적 접근통제

개인정보처리시스템에 대하여 인가되지 않는 접근 (개인정보의 불법 사용, 누출, 변조·훼손 등) 을 관리적(조직내부의 정책 또는 규정 등)인 방법으로 차단

세부 조치 사항

- 개인정보처리시스템의 개인정보 접근권한은 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여
- 개인정보취급자 변경시 지체없이 개인정보처리시스템의 접근권한 변경
- 개인정보처리시스템에 대한 권한부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소한 3년간 보관(정보통신망법 적용 기준 : 5년)

2-2. 개인정보 관리적 보호조치

물리적 접근통제

개인정보를 포함하는 파일이나 매체를 보관하고 있는 전산실이나 자료실 또는 개인영상자료를 저장하는 공간에 감시카메라와 출입통제장치를 설치하고 이에 대한 기록을 관리

개인정보 저장소 물리적 접근통제

- CCTV나 감시카메라 등의 감시장비 또는 생체인식장치나 전자출입증 등의 출입통제장치를 설치
- 출입 내역을 기록 · 관리

CCTV 모니터링실 물리적 접근통제

- 출입을 통제하는 감시장비와 출입통제장치를 설치
- 출입내역을 기록 · 관리

2-2. 개인정보 관리적 보호조치

출력·복사시 보호조치

- 개인정보 출력시 용도를 특정하고 출력항목을 최소화
- 개인정보의 종이인쇄 및 이동식 저장매체 저장시 사전 승인

출력·복사시 승인내용

- 출력·복사물 일련번호
- 출력·복사물의 형태
- 출력·복사 일시
- 출력·복사의 목적
- 출력·복사를 한 자의 소속 및 성명
- 출력·복사물을 전달받을 자
- 출력·복사물의 파기일자
- 출력·복사물의 파기 책임자

2-2. 개인정보 관리적 보호조치

개인정보 표시제한

내부 관리자에 의한 유출 예방을 위해 화면 출력 시 주요 개인정보를 마스킹하여 표시제한 조치를 취하도록 권고

표시제한 원칙

- 성명 중 이름의 첫 번째 글자 이상
- 생년월일
- 전화번호 또는 휴대폰 전화번호의 국번
- 주소의 읍·면·동
- 인터넷주소는 버전 4의 경우 17 ~ 24비트 영역,
버전 6의 경우 113 ~ 128비트 영역

2-3. 개인정보 기술적 보호조치

개인정보처리시스템의 관리

개인정보 처리 및 개인정보파일을 정보통신망으로 송수신할 때 등에 있어서
개인정보를 처리하는 시스템에 대한 안전성 확보조치 실시

- 시스템 도입 시점부터 고려
- 시스템 연계시 관계중앙행정기관과의 협의 필요

기술적 안전성 확보 조치

- 컴퓨터 바이러스 침투여부 점검
- 암호화 통신 등 개인정보를 안전하게 네트워크 상에서 전송할 수 있는 전송조치
- 침입차단시스템 등 기술적 접근통제장치의 설치 및 운영
- 전송데이터에 대한 별도 암호화나 잠금기능 사용
- 개인정보와 일반정보 보관 있어 시스템에서의 별도보관관리
- 기타 내외부적 노출, 훼손, 변조, 침입, 탐지 등에 대한 기술적 보안조치

관리적 안전성 확보 조치

- 시스템 사용자별, 업무별 접근권한 설정
[접근권한의 설정은 개인정보취급이 불가피한 자에 한해서만 최소화]
- 접근내역 기록관리(입출력사항, 수정사항, 파일별/담당자별 내역관리)
[로그파일을 이용하여 관리 가능-로그파일에 대한 분기별 1-2회 점검]

2-3. 개인정보 기술적 보호조치

개인정보처리시스템의 관리

❖ 시스템 연계시 주의사항

▪ 협의내용

- 공동이용대상 개인정보
- 공동이용대상 개인정보의 제공방법 및 정보전달 체계
- 보호대상 및 위험요소, 자원별 위험요소, 네트워크 및 인터넷 보호 대책 등 개인정보보호를 위한 조치
- 장애관리, 백업 및 복구 등을 포함한 시스템 관리 대책
- 연계시스템에 대한 책임자 지정 등



2-3. 개인정보 기술적 보호조치

기술적 접근통제(1)

개인정보처리시스템에 대하여 인가되지 않는 접근 (개인정보의 불법사용, 누출, 변조·훼손 등) 을 기술적(침입차단, 침입탐지 등) 방법으로 통제

세부 조치 사항

- 공인인증서 등의 안전한 인증방식 도입
- 개인정보처리시스템을 침입차단 및 침입탐지 기능을 포함한 시스템을 설치·운영하여 보호
- 개인정보취급자의 패스워드 작성규칙 수립 및 이행
- 개인정보처리시스템 및 개인정보취급자의 PC 설정 (P2P,공유설정 등)

2-3. 개인정보 기술적 보호조치

기술적 접근통제(2)

공공기관의 경우 기술적 보호조치 가이드라인에 따라 추가 통제 요구

세부 요구 사항

- 개인정보 처리 단말기 통제
- 웹 및 C/S 애플리케이션 통제
- 업무화면 통제
- 개인정보 이용/제공 시 전자결재
- 네트워크 접근 통제
- 웹사이트 개인정보 노출 점검 및 차단

2-3. 개인정보 기술적 보호조치

접속기록의 위·변조방지

- 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 처리일시, 처리 내역 등 접속기록을 저장하고 월 1회 이상 정기적으로 확인·감독
- 접속기록이 위·변조되지 않도록 별도 저장장치에 백업 보관

세부 조치 사항

- 개인정보처리시스템의 제반 보호에 관한 사항 확인
- 시스템 이상유무 확인 등을 위해 주기적으로 확인감독
- 감사로그(audit log)등을 위해 일정기간 이상 보존관리
- 별도 저장장치에 백업 보관

2-3. 개인정보 기술적 보호조치

개인정보의 암호화

- 비밀번호, 생체정보 등 본인임을 인증하는 정보에 대해 일방향 암호화
- 주민등록번호, 신용카드 및 계좌번호와 같은 개인정보를 외부로 송신 또는 PC에 저장시 암호화

세부 조치 사항

- 비밀번호, 생체정보(지문, 홍채 등) 등의 정보가 노출 및 위·변조되지 않도록 일방향 함수(해쉬함수) 이용 저장
- 주민번호 및 금융정보에 대한 암호화
- 정보통신망을 통해 외부로 개인정보 송수신시 암호화
- 개인용컴퓨터(PC) 또는 저장매체에 개인정보 저장 시 암호화

2-3. 개인정보 기술적 보호조치

보안서버 구축

보안서버는 정보통신망에서 패스워드, 주민번호 등의 개인정보를 암호화 (Encryption)하여 전송하는 기능을 제공하는 서버

[보안서버가 아닌 경우]



[보안서버인 경우]



이용자 개인정보 입력

2-3. 개인정보 기술적 보호조치

악성프로그램 방지

악성프로그램은 컴퓨터의 정상적인 동작을 방해하거나, 제작자의 의도에 따라 개인정보 유출 등 악성행위를 하므로 백신 소프트웨어 및 보안패치를 통한 예방 및 대응 필요

세부 조치 사항

- 백신 소프트웨어를 설치하고 월1회 이상 주기적으로 갱신점검
- 백신 소프트웨어 및 운영체제 업데이트 공지가 있는 경우 응용프로그램과 정합성을 고려하여 최신 소프트웨어로 갱신점검
- 정보보호 실천수칙 준수

2-3. 개인정보 기술적 보호조치

개인정보 파일/문서 통제

- 허용된 범위 내에서 인쇄, 복사 될 수 있도록 강력한 통제수단을 적용
- 문서 유출 등에 대한 책임 추적성을 확보

개인정보 파일 통제

- 사용자 PC에 다운로드 하는 경우 자동으로 암호화
- 디지털 문서에 DRM을 적용

인쇄/출력물 통제

- 개인정보를 종이문서로 출력하는 경우 워터마킹 기술 이용
- 해당 기관 명칭 및 로고, 일련번호, 출력기기 고유번호, 출력자 성명, 출력 시간 등을 표시

2-3. 개인정보 기술적 보호조치

개인정보 파기

PC 또는 이동형 저장매체에 보관된 개인정보를 불완전하게 파기하여 개인정보가 외부에 유출되는 것을 예방하기 위해 적절한 파기 필요

세부 조치 사항

- 개인정보가 보관된 저장매체 불용처리
- 출력물 파기
- 파기 시 접근통제 및 기록

2-4. 개인정보 위탁관리

수탁기관이 행한 개인정보보호조치는 개인정보를 보유한 공공기관이 한 것으로 간주되므로 개인정보처리 등의 사무 위탁시 철저한 관리 필요.

위탁관리 계획수립

- 위탁관리 할 개인정보처리범위와 기간 등을 정의하여 계획서 작성

위탁계약 체결

- 위탁계약시 개인정보처리관리에 있어 위탁기관이 지켜야 할 관리사항을 정의하고 책임 설정

위탁사실 공개

- 개인정보의 처리에 관한 사무를 위탁하고자 하는 경우 정보주체들이 그 사실을 알수 있도록 사전 공개

위탁기관 실태점검

- 수탁기관이 처리하고 있는 개인정보 관리사항을 정기적으로 점검

<붙임 1> 영상정보 처리기기의 설치 및 운영 제한 – 설치기준

설치 기준

범죄예방 및
수사 목적

시설안전 및
화재예방 목적

교통단속,
교통정보
수집 분석 및
제공 목적

공익
목적

※ 이외의 공개된 장소에서 CCTV 설치금지

설치 제한

- 불특정 다수가 이용하는 목욕실, 화장실, 발한실(사우나) 등 사생활 침해가 우려되는 공간

※ 예외 : 교도소, 정신보건 시설 등

<붙임 1> 영상정보 처리기기의 설치 및 운영 제한 – 설치기준

설치 및 운영 고지

설치 장소마다 정보주체가 CCTV 설치 및 운영 중임을
인지할 수 있도록 안내판을 통해 고지

고지 내용

1. 설치 목적 및 장소
2. 촬영범위 및 시간
3. 관리책임자 및 연락처

고지 위치

- 출입구 등 정보주체가 쉽게 인지할 수 있는 위치 및 장소

CCTV 설치 및 운영 안내판 예제

CCTV 설치 안내문

- 범죄예방과 학생의 안전을 위해
CCTV가 24시간 작동하고 있습니다.
- 촬영범위 : 360°회전 100m이내지역
- CCTV운영과 관련된 문의사항은
OO초등학교 행정실로 연락주시기 바랍니다.

서울 OO초등학교 행정실 00) 0000-0000

<붙임 1> 영상정보 처리기기의 설치 및 운영 제한 – 설치기준

운영 및 관리 지침 마련

처리기기 운영 및 관리 지침 마련

- 설치 근거 및 목적
 - 설치 대수, 위치, 촬영범위 및 성능
 - 관리 책임자, 담당부서 및 접근 권한자
 - 녹화시간
 - 녹화기록의 보관(장소), 관리, 폐기 방법
 - 전송되는 정보의 모니터링 방법 및 장소
 - 영상 개인정보보호를 위한 기술적, 관리적 보호조치 등
- ※ 개인정보보호를 위한 관리적·기술적·물리적 보호조치 적용

업무 위탁

수탁기업 내 필수사항

- 개인정보 보호에 필요한 장비 및 기술 보유
- 수탁자 내부 전문인력 보유
- 위탁대상이 되는 사무 범위
- 정보 접근 제한 등을 기재

〈참고〉 법 위반 사례 및 조치사항 (DON'Ts & DOSs)



(1) 개인정보 수집 · 이용 · 제공 동의

DON'Ts (위반사례)

- 멤버십 가입 신청 시 수집 · 이용 목적, 수집항목, 보유기간 등에 대한 정보주체의 동의 항목 누락
- 14세 미만 아동에 대한 개인정보 수집 시 법정대리인 동의절차 누락
- 민감정보, 고유식별정보 수집 시 별도동의 미획득
- 정보주체의 별도 동의없이 홍보, 판매를 위해 개인정보 무단 활용
- 정보주체 동의없이 이벤트를 위한 개인정보 제3자 제공

DOs (조치사항)

- ▶ 개인정보 수집에 따른 동의항목 확인
- ▶ 만 14세 미만의 아동 정보를 처리 하기 위해 법정대리인의 동의 필요
- ▶ 민감정보, 고유식별정보 수집 시 별도동의 획득 필요
- ▶ 홍보, 판매 등 목적외 이용제공을 위한 별도동의 획득 및 고지 필요
- ▶ 개인정보 목적외 제3자 제공 시 별도동의 획득 필요

(2) 최소정보 수집

DON'Ts (위반사례)

- A사는 인터넷을 통한 신발 판매 시 주민번호, 직장정보, 소득, 자녀정보 등 필수정보와 선택정보를 구분하지 않고 포괄 동의 후 수집

이름

주민번호

주소

핸드폰번호

유선번호

직장명

직장주소

연소득

주거형태

배우자 정보

취미

The screenshot shows a web form with multiple input fields. The fields are organized into sections, with some fields highlighted in red. The fields include: 이름 (Name), 주민번호 (Resident Number), 주소 (Address), 핸드폰번호 (Mobile Number), 유선번호 (Landline Number), 직장명 (Company Name), 직장주소 (Company Address), 연소득 (Annual Income), 주거형태 (Residence Type), 배우자 정보 (Spouse Information), and 취미 (Hobbies). The form also contains checkboxes for consent and other options.

DOs (조치사항)

- ▶ 신발 판매를 위한 필수정보와 부가적인 정보(선택정보)를 구분하여 동의 획득하고, 부가정보 수집에 동의하지 않은 이유로 서비스 제공 거부 금지

“주민번호, 직장정보, 소득, 주거형태 등의 정보는 최소정보인가?”

- ▶ 수집하는 개인정보가 최소정보라는 것은 개인정보처리자가 입증
- ▶ 개인정보처리자는 정보주체가 필요 최소한의 정보 외의 개인정보 수집에 동의하지 않는다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부할 수 없음(과태료 3천만원)

(3) 민감정보 및 고유식별정보 수집을 위한 별도 동의

DON'Ts (위반사례)

고유식별정보에 대한 무단 수집

* 회원가입을 위한 필수항목입니다.

- 이름
- 주민등록번호 -
- 여권번호
- 자동차등록번호
- 전화번호

민감정보에 대한 무단 수집

* 회원가입을 위한 필수항목입니다.

- 종교
- 본인병력
- 가족병력
- 지지하는 정당

DOs (조치사항)

- 고유식별정보 및 민감정보는 내용적으로 수집이 금지되고, 필요 시 별도의 동의 획득 필요

The image shows three screenshots of a web form, each with a consent checkbox and a '동의하지 않음' (Do not consent) button.

- 0000의 개인정보 수집 및 이용**
 수집 및 이용목적 동의 동의하지 않음
 <일반동의>
- 0000의 민감정보 추가수집**
 민감정보 추가수집 동의 동의하지 않음
 <별도동의>
- 0000의 고유식별정보 수집 동의**
 고유식별정보 수집 동의 동의하지 않음
 <별도동의>

(4) 업무 위탁, 영업양도에 따른 공개 및 고지

일반 위탁 시 공개 예시

**전자 패밀리 서비스 이행을 위해 개인정보 취급 업무 중 일부를 아래와 같이 외부 전문 업체에 위탁하여 운영하고 있습니다.

위탁업체	위탁업무 내용
AAA	회원제 서비스 이용에 따른 본인 실명 확인
BBB	온라인 광고, 캠페인 집행을 위한 위탁- 광고, 이벤트 등과 같은 마케팅 업무 수행에 필요한 고객 정보 추출, 활용
CCC	마케팅 업무 운영 대행을 위한 위탁- 이벤트 당첨자 상품 배송을 위한 고객정보 추출, 제품/기업 및 이벤트 홍보 메일전송을 위한 고객정보추출등과 같은 마케팅 업무 운영
DDD	고객 응대 업무 효율성 제고를 위한 위탁 - **전자 패밀리 회원 고객문의 응대, 물품 구매관련 및 배송관련 고객 문의 응대, 만족도 조사(제품구매,배송설치,서비스)
EEE	제품 구매에 따른 물품 배송 및 제품설치

홍보·판매 위탁·양도 시 고지 예시

- 재화 또는 서비스 홍보 · 판매 업무를 위탁하는 경우에는 업무의 내용, 수탁자를 고지

당사의 서비스 이행을 위해 아래와 같이 개인정보 취급업무를 위탁함
 ○ 취급위탁을 받는 자 : A 텔레마케팅
 ○ 취급위탁 내용 : oo제휴상품 홍보 및 안내

- 영업의 양도 합병으로 개인정보를 이전하는 경우에는 이전 사실, 양수자의 성명, 주소, 전화번호 및 그 밖의 연락처, 이전을 원하지 않는 경우 조치방법 및 절차 등을 고지

당사는 2011년 1월 1일자로 oo사업 및 홈페이지 운영을 B사에 양도함에 따른 개인정보 이전 안내
 ○ 영업양도로 이전 ○ 양수자(김**), oo구 00동, 전화 121-4567, 팩스 02-232-5678
 ※ 개인정보 이전을 원하지 않는 경우 당사 홈페이지에서 회원탈퇴 가능

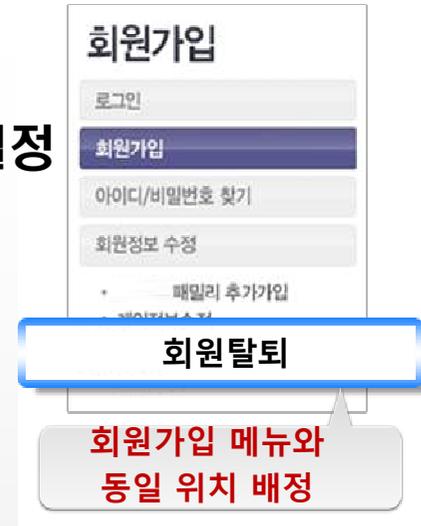
(5) 개인정보의 파기 및 회원탈퇴

DON'Ts (위반사례)

- A호텔은 웹사이트 내 회원가입 화면에 회원탈퇴 메뉴가 없어 회원탈퇴가 어려움
- B사는 회원탈퇴를 요청한 회원의 정보를 파기하지 않고, 탈퇴 요청한 회원에 광고 메일 전공

DOs (조치사항)

- ▶ 회원가입 화면에 회원탈퇴 메뉴 설정
관련된 회원정보 즉시 파기



- ▶ 개인정보의 처리목적 달성 등 개인정보가 불필요해진 경우 개인정보를 지체없이 파기
- 복구 또는 재생이 불가능하도록 파기(종이 세단기 분쇄, 소거 S/W 사용 데이터 파기 등)

(6) 안전성 확보조치

DON'Ts (위반사례)

- A사는 개인정보 내부관리계획을 작성하였으나, 개인 컴퓨터에 보관
- B영업점은 주민번호, 비밀번호 등을 암호화하지 않은 상태로 보관하다가 외부 해킹으로 개인정보 유출
- C사는 내부직원에 의해 개인정보가 유출되었으나, 개인정보 접근 사실을 기록하지 않아 유출자를 확인할 수 없음
- D사는 퇴직한 직원의 접근권한을 폐기하지 않아, 퇴직 후 시스템에 접근하여 개인정보 유출

DOs (조치사항)

- ▶ 개인정보 내부관리계획을 작성하여 개인정보 보호책임자의 결재를 거쳐 시행
- ▶ 주민번호 등 고유식별정보, 비밀번호, 생체정보는 전송 시 암호화하고, 인터넷망과 DMZ (중간구간) 저장 시에는 암호화
- ▶ 내부직원의 개인정보 DB 접속 시 일시, IP주소, 접속자 성명 등 접속기록을 보관 조치
- ▶ 퇴직한 직원의 ID, PW를 제거하여 불법적인 접근 차단

감사합니다.