

앱 개발자를 위한 개인정보보호 안내서

2012. 3



CONTENTS



개인정보보호 바로알기

- 1 개요 / 4
- 2 개인정보의 정의 / 5
- 3 개인정보의 유형 / 5
- 4 법률의 이해 / 7



앱 개발 준비하기

- 1 개인정보 수집 최소화하기 / 11
- 2 신뢰할 수 있는 앱 개발 툴 이용하기 / 11
- 3 Secure coding 적용하기 / 12
- 4 앱 서비스 보안대책 마련하기 / 13
- 5 개인정보보호 관련 법률 검토하기 / 14



3장

법규준수하여 앱 개발하기

- 1 개인정보취급방침 공개하기 / 15
- 2 개인정보 수집 및 이용에 대한 동의 획득하기 / 16
- 3 민감한 개인정보는 수집하지 않기 / 19
- 4 개인정보 취급위탁시 이용자에게 알리고 동의 획득하기 / 20
- 5 개인정보 제3자 제공시 이용자에게 알리고 동의 획득하기 / 21
- 6 미성년자 개인정보 수집시 법정대리인 동의 획득하기 / 23
- 7 주민등록번호의 사용 제한 / 24
- 8 개인정보 수집 목적에 대해서만 이용하기 / 25
- 9 회원정보 열람·정정 등 이용자 권리 보장하기 / 25
- 10 개인정보 즉시 파기하기 / 26
- 11 기술적 보호조치 구현하기 / 28





개인정보보호 바로알기



1 개요

스마트폰, 태블릿 PC 등 스마트 기기의 대중화와 함께 앱(App) 이용이 증가함에 따라, 이를 통한 개인정보 유·노출 위험성 또한 높아지고 있다.

앱을 통한 개인정보 유·노출 등의 피해를 최소화하기 위해서는 앱 개발단계에서부터 개인정보보호 조치가 이루어져야 한다.

본 안내서는 개인정보보호에 대한 앱 개발자와 서비스 제공자의 이해를 높이고, 앱 개발시 고려해야할 개인정보보호 관련 법률준수 사항을 안내하기 위해 개발되었다.

본 안내서는 앱 개발시 준수해야할 사항을 개인정보보호 관련 법률과 함께 설명하고 이에 대한 예시화면을 제공함으로써, 앱 개발자와 서비스 제공자가 참조할 수 있도록 하였다.

앱 개발시 준수해야할 개인정보보호 관련 법률

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)
- 위치정보의 보호 및 이용 등에 관한 법률(이하 위치정보보호법)

※ 적용범위 : 이용자의 개인정보가 서비스 제공자에게 전송·수집되는 경우에는 개인정보보호 관련 법률을 준수해야 하며, 개인정보의 전송·수집 없이 스마트 기기내에서만 처리되는 경우에는 적용범위에서 제외될 수 있다.

2 개인정보의 정의

개인정보는 “①생존하는 개인에 관한 정보로써 ②특정 개인을 식별하거나 식별할 수 있는 모든 정보”를 말한다.

① 생존하는 개인에 관한 정보

개인정보의 주체가 현재 생존하는 자연인(自然人)에 관한 정보이어야 함을 말하며 법인(法人) 또는 단체의 정보는 해당되지 않는다. 다만, 사망한 자의 정보라 할지라도 생존하는 유족 등 후손과 관련이 있으면 후손의 개인정보로서 보호대상이 될 수 있다.

② 식별하거나 식별 할 수 있는 정보

개인정보로 인정되기 위해서는 해당 정보가 특정 개인을 식별하거나 식별 가능하여야 함을 말한다. 해당 정보만으로 개인을 식별할 수 있는 정보뿐만 아니라 다른 정보와 용이하게 결합해서 개인 식별이 가능한 경우의 정보도 개인정보로 규정하고 있다.

예를 들어, 주민등록번호는 개인마다 고유한 것이므로 개인정보로 활용될 수 있다. 하지만, 성명과 같은 정보는 개인마다 고유하지 않고 동일한 유형에 속하는 사람이 많기 때문에 그 정보 하나만으로는 개인정보로 보기 어렵다. 그러나, 성명이 주민등록번호나 주소 등의 정보와 결합되는 경우에는 특정 개인을 식별할 수 있어 개인정보로 볼 수 있다.

3 개인정보의 유형

개인정보는 주민등록번호 등 직접적으로 개인을 식별할 수 있는 정보뿐만 아니라 나이, 사상, 학력, 구매내역 등과 같이 해당 정보만을 이용해서는 개인을 식별할 수 없지만, 다양한 정보와 결합·조합하여 개인을 식별할 수 있다면 해당 정보 또한

개인정보에 포함된다.

앱 서비스의 경우, 회원가입 절차 등을 통해 수집한 이용자의 주민등록번호 등의 직접적인 개인정보 뿐만 아니라, 서비스 이용 과정에서 생성되는 통화내역, 로그기록, 구매내역 등도 다른 정보와 결합·조합하여 개인을 식별할 수 있다면 개인정보로 취급해야 한다.

개인정보로 취급될 수 있는 정보의 유형과 그 구체적인 예는 다음과 같다. 특히, 위치 정보의 경우 개인위치정보 유출·오용·남용시 개인의 생명 및 신체에 즉각적인 위험을 초래할 수 있어 별도의 법률(위치정보보호법)로 규정하고 있다.

유형	개인정보로 취급될 수 있는 정보의 예
인적정보	성명, 주민등록번호, 주소, 본적지, 연락처, 생년월일, 이메일 주소, 사진, 가족 관계 및 가족구성원 정보 등
신체적정보	(신체정보) 얼굴, 지문, 홍채, 음성, 유전자정보, 키, 몸무게 등 (의료/건강정보) 건강상태, 진료기록, 신체장애, 장애등급, 병력 등
정신적정보	(기호/성향정보) 도서·비디오 등 대여기록, 잡지구독정보, 물품구매내역, 웹사이트 검색내역 등 (내면의 비밀 등) 사상, 신조, 종교, 가치관, 정당·노조 가입여부 및 활동내역 등
재산적정보	(개인금융정보) 소득, 신용카드번호, 통장계좌번호, 동산·부동산 보유내역, 저축내역 등 (신용정보) 신용평가정보, 대출 또는 담보설정 내역, 신용카드 사용내역 등
사회적정보	(교육정보) 학력, 성적, 출결상황, 자격증 보유내역, 상벌기록 등 (법적정보) 전과·범죄 기록, 재판 기록, 과태료 납부내역 등 (근로정보) 직장, 근무처, 근로경력, 상벌기록, 직무평가기록 등 (병역정보) 병역여부, 군번, 계급, 근무부대 등
스마트 기기에서 개인정보로 취급될 수 있는 정보의 예	
전화번호, 주소록, 통화내역, 위치정보, SMS, 사진, 동영상, 브라우저 접근기록, 캘린더, USIM 카드 일련번호 등	

4 법률의 이해

① 기본원칙

개인정보보호를 위한 기본 원칙은 이용자의 ‘개인정보 자기결정권’을 보장하는 것이다.

이용자의 개인정보 자기결정권

- 누가 어떤 목적으로 자신의 개인정보를 수집하고 이용는지 정보 제공 이전에 명확하게 인지하고
- 언제든지 자신의 개인정보를 열람·정정할 수 있으며
- 개인정보 이용을 원하지 않을 경우, 이용에 대한 동의철회 또는 파기를 요청할 수 있는 권리를 보장받아야 한다.

위와 같은 이유로, 앱 개발자는 이용자의 개인정보를 수집·이용·제공할 때에는 “이용자에게 그 사실을 알리고 동의를 받도록 하며 목적이 달성되었으면 해당 정보를 파기”하도록 구현해야 한다.

② 보호대상

이용자의 개인정보가 보호되어야 하며, 이용자란 “사업자가 제공하는 서비스를 이용하는 자”를 의미한다.

이용자 유형

- 온라인 회원같이 계속적으로 서비스를 이용하는 경우
- 일회성 또는 비정기적으로 서비스를 이용하는 경우

다시 말해, 앱을 통해 개인정보를 수집·이용하는 경우에는 해당 앱을 이용하는 이용자의 개인정보가 보호대상이 된다.

③ 적용대상

개인정보보호 규정은 “정보통신망법의 정보통신서비스제공자”와 “위치정보보호법의 위치정보사업자 및 위치기반서비스사업자”에 대해 적용된다.

개인정보보호 규정의 적용대상

- 정보통신서비스제공자 : 유·무선 통신망을 통하여 정보제공 또는 매개하는 자를 말하며, 앱 서비스를 제공하는 자는 정보통신서비스제공자에 해당된다.
 - 이동통신사업자, 포털사업자, 쇼핑몰사업자 등
- 위치정보사업자 : 위치정보를 수집하여 위치기반서비스사업자에게 위치정보를 제공하는 자를 말한다.
 - 이동통신사업자, 단말기OS제조사 등
- 위치기반서비스사업자 : 위치정보사업자로부터 위치정보를 전송(제공)받아 이용자에게 서비스를 제공하는 자를 말하며, 위치정보를 활용한 앱 서비스를 제공하는 자는 위치기반서비스사업자에 해당된다.
 - 친구찾기 앱, 물류 앱, 지도안내 앱 등

④ 법규 및 벌칙조항

앱 개발자는 개인정보보호와 관련된 주요 법률과 위반시 벌칙조항을 숙지하고 위반하지 않도록 주의해야 한다.

구 분	주요 내용	벌칙
개인정보 수집·이용·제공	○ 개인정보 취급방침 공개(정보통신망법 제27조의2)	2천만원 이하 과태료
	○ 개인위치정보 수집·이용·제공 관련 사항을 이용약관에 명시(위치정보보호법 제18조 및 제19조)	1천만원 이하 과태료
	○ 필요 최소한의 개인정보만을 수집(정보통신망법 제23조)	1천만원 이하 과태료
	○ 이용자가 필요 최소한의 개인정보 이외의 정보를 미제공한 다는 이유로 서비스 거부 금지(정보통신망법 제23조)	3천만원 이하 과태료
	○ 개인정보 수집·이용시 동의 획득(정보통신망법 제22조)	5년이하 징역 또는 5천만원 이하 벌금

구 분	주요 내용	벌칙
개인정보 수집·이용 ·제공	○ 민감한 개인정보 수집시 동의 획득(정보통신망법 제23조)	5년이하 징역 또는 5천만원 이하 벌금
	○ 개인정보 제3자 제공시 동의 획득(정보통신망법 제24조의2)	5년이하 징역 또는 5천만원 이하 벌금
	○ 개인정보 취급 위탁시 동의 획득(정보통신망법 제25조)	5년이하 징역 또는 5천만원 이하 벌금
	○ 제3자 제공 및 취급위탁은 개인정보 수집·이용 동의와 구분 하여 동의 획득. 미동의시 서비스 제공 거부 금지 (정보통신망법 제24의2)	1천만원 이하 과태료
	○ 개인위치정보 수집·이용·제공시 이용약관에 따른 동의 획득 (위치정보보호법 제18조 및 제19조)	5년이하 징역 또는 5천만원 이하 벌금
	○ 개인위치정보를 개인위치정보주체가 지정하는 제3자 제공시 제공받는 자, 제공일시 및 제공목적 등을 고지 및 동의 획득 (위치정보보호법 제19조)	1천만원 이하 과태료
	○ 14세 미만 아동은 법정대리인 동의 획득 (정보통신망법 제31조)	5년이하 징역 또는 5천만원 이하 벌금
	○ 14세 미만 아동은 법정대리인 동의 획득 (위치정보보호법 제25조)	1천만원 이하 과태료
	○ 동의 받은 목적과 다른 목적으로 개인정보 이용 금지 (정보통신망법 제24조)	5년이하 징역 또는 5천만원 이하 벌금
	○ 개인위치정보 수집·이용·제공 사실을 이용약관에 명시 또 는 고지한 범위를 넘어 이용하거나 제3자 제공 금지 (위치정보보호법 제21조)	5년이하 징역 또는 5천만원 이하 벌금
개인정보 관리	○ 개인위치정보를 개인위치정보 주체가 지정하는 제3자 제공 시 매회 제공내역 즉시통보(위치정보보호법 제19조)	1천만원 이하 과태료
	○ 주민등록번호의 사용 제한 (정보통신망법 제23조의2)	3천만원 이하 과태료
	○ 개인정보 보호조치 수행(정보통신망법 제28조)	3천만원 이하 과태료
개인정보 관리	○ 위치정보 보호조치 수행 및 위치정보 수집·이용·제공사실 기록보존(위치정보보호법 제16조)	1년이하 징역 또는 2천만원 이하 벌금
	○ 개인정보 보호조치 미수행으로 개인정보 유출 (정보통신망법 제28조)	2년이하 징역 또는 1천만원 이하 벌금

구 분	주요 내용	벌칙
개인정보 파기	○ 지체없이 개인정보 파기(정보통신망법 제29조)	3천만원 이하 과태료
	○ 지체없이 개인위치정보 파기(위치정보보호법 제23조)	1년이하 징역 또는 2천만원 이하 벌금
이용자 권리	○ 이용자 동의철회, 열람·정정 요구 방법 마련 및 조치 (정보통신망법 제30조)	3천만원 이하 과태료
	○ 개인위치정보 수집·이용·제공에 대한 일시중지 요구 처리 및 수단 제공(위치정보보호법 제24조)	2천만원 이하 과태료
	○ 개인정보 오류정정 요구시 지체없이 처리한 후 개인정보 제공·이용(정보통신망법 제30조)	5년이하 징역 또는 5천만원 이하 벌금
	○ 개인위치정보 수집 등에 대한 열람·고지·정정 요구 처리 (위치정보보호법 제24조)	1천만원 이하 과태료
기타	○ 위치정보사업 허가(위치정보보호법 제5조)	5년이하 징역 또는 5천만원 이하 벌금
	○ 위치정보사업 변경허가·신고(위치정보보호법 제5조)	3년이하 징역 또는 3천만원 이하 벌금
	○ 위치기반서비스사업 신고(위치정보보호법 제9조)	3년이하 징역 또는 3천만원 이하 벌금
	○ 위치기반서비스사업 변경신고(위치정보보호법 제9조)	1년이하 징역 또는 2천만원 이하 벌금
	○ 위치정보 이용약관 신고(위치정보보호법 제12조)	1천만원 이하 과태료
	○ 위치정보 이용약관 변경신고(위치정보보호법 제12조)	1천만원 이하 과태료

2장

앱 개발 준비하기



1 개인정보 수집 최소화하기

앱을 통해 개인정보 수집시 최소한의 개인정보만을 수집해야한다. 앱 설계 시 ①서비스에 필요한 개인정보 종류를 조사하고, ②서비스를 위해 필수 수집해야 하는지 또는 미수집해도 되는지 여부를 검토해야한다. ③수집하는 개인정보는 필수 및 선택항목으로 구분하고 이용자가 선택항목을 입력하지 않는다고 해서 서비스 이용을 금지해서는 안된다. 특히, 모든 개인정보를 회원가입시 일괄 수집하지 않도록 하고, 필요한 시점에 수집하도록 한다.

① 앱 설계 시,
서비스에 필요한
개인정보 전체 조사

② 서비스 이용에 꼭
필요한 개인정보
인지 검토(최소 수집)

③ 필수 및 선택
개인정보로 구분하여
수집

2 신뢰할 수 있는 앱 개발 툴 이용하기

앱 개발시 신뢰할 수 있는 앱 개발 툴(API, SDK 등)을 이용해야 한다. 출처를 알 수 없는 개발 툴 이용시, 개인정보 유·노출 위험이 있으므로 주의해야 한다. 신뢰된 개발 툴 이용시에도 주요기능, 취급하는 개인정보 등을 검토하여 불필요한 개인정보 수집·이용을 최소화해야 한다.



Tip

앱 개발과 관련된 Open API, S/W모듈 등에 관한 자세한 사항은 방송통신위원회와 한국인터넷진흥원에서 운영하는 ‘스마트 모바일 앱 개발 지원센터(www.smac.or.kr)’ 홈페이지 참조

① 국내/외 Open API

- 공공, 포털, 이통사, 기타 등

② S/W모듈

- 운영체제별(iPhone, android, Windows phone, 기타 운영체제 등)
- 이용형태별(그래픽소스, 멀티미디어, 프로그래밍, 기획/마케팅, 이용형태 등)

또한, 앱스토어나 OS업체가 운영하는 ‘개발자 지원 홈페이지’ 참조

① SKT(dev.tstore.co.kr)② KT(seller.ollehmarket.com)③ LG U+(devpartner.lguplus.co.kr)④ 구글(developer.android.com)⑤ 애플(developer.apple.com)

3 Secure Coding 적용하기

앱 개발자는 소스코드상 취약점을 최소화하기 위해 노력해야 한다. 소스코드의 안전성을 확보하여 해킹 등을 통한 개인정보 유·노출 사고발생을 최소화할 수 있다. 앱 개발자는 소스코드상의 취약점을 최소화하기 위해 Secure Coding을 적용해 앱을 개발해야 한다.



Tip

Secure Coding 가이드라인(국내)에 대한 세부 내용 및 개발 방법은 ‘행정안전부 홈페이지(www.mopas.go.kr)»정책자료»참고자료실’ 참조

① 정보시스템 SW 개발보안 가이드

- JAVA 시큐어 코딩 가이드
- C 시큐어 코딩 가이드
- Android-JAVA 시큐어 코딩 가이드

이외, 국외의 Secure Coding 가이드라인은 아래를 참조

- ① CERT Secure Coding Standards(www.cert.org»Developers)
 - The CERT Oracle Secure Coding Standard for Java
 - The CERT C Secure Coding Standard
 - The CERT C++ Secure Coding Standard
- ② Secure Coding Guide(developer.apple.com)

4 앱 서비스 보안대책 마련하기

앱 개발자와 서비스 제공자는 서비스 전반에 대한 보안대책을 마련해야 한다. 데이터 전송구간 및 시스템 등에 대한 보안대책 미적용시, 해당 취약점을 통해 개인정보가 유출될 수 있다. 앱 개발자와 서비스 제공자는 개인정보보호 관련 보호기준 등을 적용함으로써 서비스 전반의 보안대책을 수립할 수 있다.



정보보호시스템 운영 및 개인정보보호 관련 보안대책 세부방법은 '한국인터넷진흥원 홈페이지 (www.kisa.or.kr)»자료실' 참조

- ① 개인정보보호 관련 보호기준
 - 개인정보의 기술적·관리적 보호조치 기준 및 해설서
 - 위치정보보호를 위한 관리적·기술적 보호조치 권고 및 해설서
 - I-PIN 2.0 도입 안내서 등
- ② 정보보호 시스템 운영 관련 보안대책
 - 보안서버구축 안내서
 - 패스워드선택 및 이용 안내서
 - 암호이용/암호기술 구현 안내서
 - 와이브로 보안기술 안내서
 - 암호 알고리즘 및 키 길이 이용 안내서
 - 스마트폰 백신 이용 안내서 등

5 개인정보보호 관련 법률 검토하기

앱이 개인정보와 위치정보를 수집·이용·제공할 경우, 정보통신망법과 위치정보보호법을 준수해야 한다.(제1장 4.법률의 이해 참조) 앱 개발자는 서비스 형태에 따라 준수해야 하는 법률을 검토하고 앱 개발시 반영해야 한다.



Tip

개인정보보호 관련 법률의 세부내용은 '한국인터넷진흥원 홈페이지(www.kisa.or.kr)»자료실, (privacy.kisa.or.kr)»기업자료실' 참조

- ① 정보통신서비스제공자를 위한 개인정보보호 가이드
- ② 위치정보의 보호 및 이용 등에 관한 법률 해설서

법규준수하여 앱 개발하기



1 개인정보취급방침 공개하기

이용자가 알아야 할 개인정보보호에 관한 사항을 ‘개인정보취급방침’으로 정하여 공개해야 한다.

※ 관련근거 : 정보통신망법 제27조의2(개인정보 취급방침의 공개)



개인정보취급방침에 포함될 세부 내용 및 작성 방법은 '한국인터넷진흥원 홈페이지(guide.kisa.or.kr)'에서 '개인정보취급방침 작성 예시' 참조

예시화면

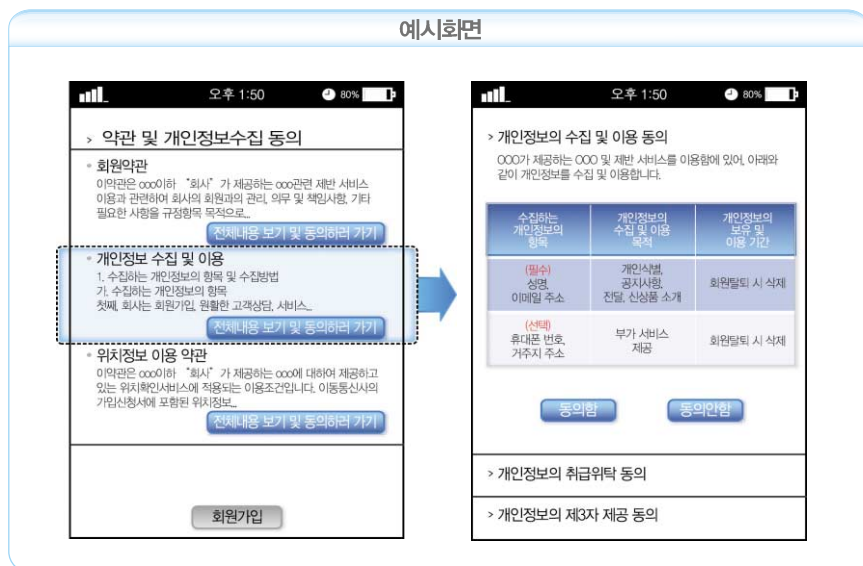


개인정보 취급방침은 이용자가 언제나 쉽게 확인할 수 있도록 앱 실행시 첫 화면에 공개하며, 링크 기능을 통해 전문을 볼 수 있도록 구현한다.

2 개인정보 수집 및 이용에 대한 동의 획득하기

이용자의 개인정보를 수집 및 이용하는 경우 이용자에게 동의를 획득해야 한다. 일정한 이벤트 또는 비회원에게 서비스를 제공하기 위한 개인정보 수집도 포함된다.

※ 관련근거 : 정보통신망법 제22조(개인정보의 수집·이용 동의 등)



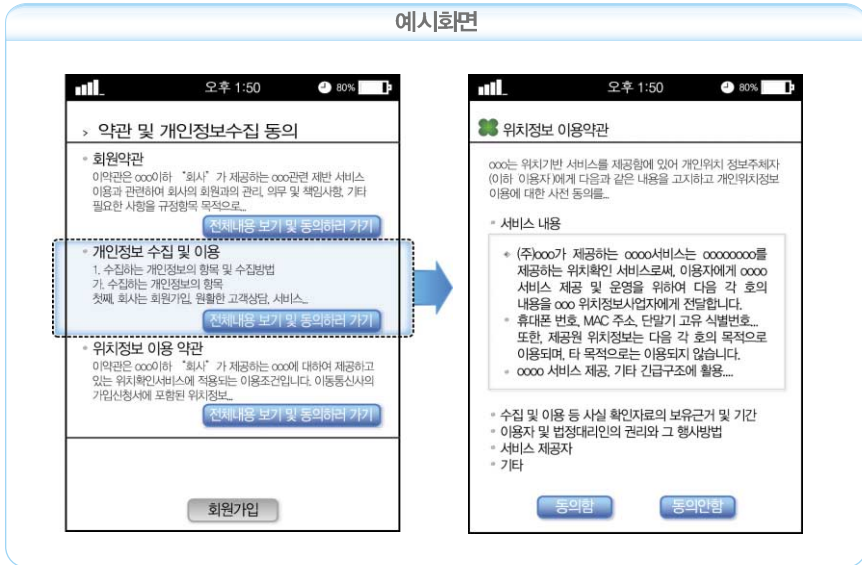
개인정보 수집 및 이용에 대한 동의 획득시, 어떤 개인정보를 왜 수집하고 언제까지 보유할 것인지에 대해 이용자가 쉽고 명확하게 인지할 수 있어야 한다. 예시화면과 같이 3가지 항목을 별도로 안내하고 동의를 획득하는 절차를 마련한다.

- ① 수집하는 개인정보의 항목(예 : 성명, 이메일주소 등)
- ② 개인정보의 수집·이용목적(예 : 정보제공, 물품배송 등)
- ③ 개인정보의 보유 및 이용 기간(예 : 회원탈퇴시 지체없이 파기)

위치정보사업자 및 위치기반서비스사업자가 개인위치정보를 수집·이용·제공하기 위해서는 위치정보 이용약관을 통해 이용자로부터 동의를 획득해야 한다.

※ 관련근거 : 위치정보보호법 제18조(개인위치정보의 수집)

위치정보보호법 제19조(개인위치정보의 이용 또는 제공)



이용약관에는 ①서비스 내용, ②개인위치정보 수집 및 이용 등 사실 확인자료의 보유근거 및 보유기간, ③이용자 및 법정대리인의 권리와 그 행사방법, ④사업자의 상호, 주소, 전화번호 등 서비스 제공자 정보 ⑤ 이외의 개인위치정보 보호를 위하여 필요한 사항이 포함되어야 한다.

또한, 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용·제공할 경우에도 이
용자 또는 소유자의 동의를 획득해야 하며, 위치정보 이용약관이나 별도의 팝업창을
통해 동의를 획득할 수 있다.

※ 관련근거 : 위치정보보호법 제15조(위치정보의 수집 등의 금지)



Tip

〈위치정보란?〉

이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 전기통신설비 및 전기통신회선설비(휴대전화, GPS 등)를 이용하여 수집

〈개인위치정보란?〉

특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것도 포함)를 의미

알고가기

〈위치정보사업 허가〉

위치정보사업을 하고자 하는 자(위치정보사업자)는 위치정보보호법 제5조에 따라 방송통신위원회에 허가를 받아야 한다. 허가를 받은 사항 중 위치정보시스템을 변경(그 변경으로 개인위치정보 보호를 위한 기술적 수준이 허가받은 때보다 저하되는 경우에 한한다)하려는 경우에는 방송통신위원회의 변경허가를 받아야 하고, 상호 또는 주된 사무소의 소재지를 변경하려는 경우에는 방송통신위원회에 변경신고를 하여야 한다.

〈위치기반서비스사업 신고〉

위치기반서비스사업을 하고자 하는 자(위치기반서비스사업자)는 위치정보보호법 제9조에 따라 방송통신위원회에 신고하여야 한다. 신고한 사항 중 상호, 주된 사무소의 소재지 또는 위치정보시스템을 변경(변경으로 인하여 개인위치정보 보호를 위한 기술적 수준이 신고한 때보다 저하되는 경우에 한한다)하고자 하는 때에는 방송통신위원회에 변경신고를 하여야 한다.

단, 위치정보가 스마트기기에서만 활용되고 사업자 서버로 전송되지 않는다면 위치기반서비스사업 신고대상에서 제외된다. 위치정보가 사업자 서버로 전송되는 경우에는 위치정보의 서버 저장기간과 상관없이 신고대상이 된다.

〈위치정보 이용약관 신고〉

위치정보사업자 및 위치기반서비스사업자는 위치정보보호법 제12조에 따라 사업개시 30일 전까지 방송통신위원회에 위치정보 이용약관을 신고해야 한다. 이용약관이 변경될 때에도 신고하여야 한다.

* 사업 허가·신고 방법 및 세부 내용은 '방송통신위원회 홈페이지(www.kcc.go.kr) > 정책/정보센터 > 자료마당 > 사업자제출자료' 참조

3 민감한 개인정보는 수집하지 않기

원칙적으로 민감한 개인정보 수집은 금지한다. 부득이하게 민감한 개인정보를 수집할 경우에는 반드시 이용자 동의를 획득해야 한다.

※ 관련근거 : 정보통신망법 제23조(개인정보의 수집 제한 등)

Tip

<민감한 개인정보란?>

과거 병력, 장애여부, 인종 및 민족, 사상, 출신지, 정치적 성향, 범죄기록, 성생활 관련 정보 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 말한다.

예시화면

민감한 개인정보는 이용자의 동의를 받거나 다른 법률에 따라 수집이 허용된 경우에 한해 수집할 수 있으며, 예시화면과 같이 다른 개인정보와 구분하여 표시하도록 한다.

4 개인정보 취급위탁시 이용자에게 알리고 동의 획득하기

개인정보 취급업무를 위탁할 경우 누구에게, 왜 주는지에 대해 이용자 동의를 획득해야 한다. 단, 이용자와 계약을 맺은 서비스를 제공하기 위해 불가피하게 발생하는 위탁 업무에 대해서는 동의획득 없이 고지나 통지로 갈음할 수 있다.

※ 관련근거 : 정보통신망법 제25조(개인정보의 취급위탁)



〈취급위탁이란?〉

사업자가 자신의 업무와 직·간접적으로 관련된 업무를 수행하기 위해 개인정보의 수집·보관·처리·이용·제공·관리·파기 등의 취급업무를 제3자에게 위탁하는 것

- 예 : 텔레마케팅을 외부 업체에 아웃소싱, 고객만족도 조사를 위해 리서치 업체 이용, 이벤트 또는 행사 개최를 대행사에 아웃소싱

예시화면

오후 1:50 80%

> 약관 및 개인정보수집 동의

- 회원약관
이약관은 000이하 "회사"가 제공하는 000관련 제반 서비스 이용과 관련하여 회사의 회원과의 권리, 의무 및 책임사항, 기타 필요한 사항을 규정함을 목적으로 함.
- 개인정보 수집 및 이용
1. 수집하는 개인정보의 항목 및 수집방법
가. 수집하는 개인정보의 항목
첫째, 회사는 회원가입, 원활한 고객상담, 서비스, ...
- 위치정보 이용 약관
이약관은 000이하 "회사"가 제공하는 000에 대하여 제공하고 있는 위치확인서비스에 적용되는 이용조건입니다. 이동통신사의 가입신청서에 포함된 위치정보...

전체내용 보기 및 동의하러 가기

회원가입

오후 1:50 80%

> 개인정보의 수집 및 이용 동의

> 개인정보의 취급위탁 동의

000는 서비스 이행을 위해 아래와 같이 개인정보 취급업무를 외부 전문업체에 위탁하여 운영하고 있습니다.

개인정보 취급위탁을 받는자(수탁자)	개인정보 취급위탁을 하는 업무의 내용
000서비스	실명확인서비스
000채배	물품배송 서비스
000시스템	고객정보 DB 시스템 운영

동의함

동의안함

> 개인정보의 제3자 제공 동의

취급위탁시 예시화면과 같이 ①개인정보 취급을 위탁받는 자(수탁자)와 ②취급위탁의 업무 내용에 대해 이용자에게 알리고 동의를 획득하면 된다. 취급위탁 업체가

많을지라도 해당 업체를 모두 명시하여야 한다. 특히, 취급위탁 동의는 개인정보의 수집·이용이나 제3자 제공과는 별도로 동의를 받아야 하며, 이에 동의하지 아니한다는 이유로 서비스 제공을 거부해서는 안된다.

5 개인정보 제3자 제공시 이용자에게 알리고 동의 획득하기

이용자의 개인정보를 제3자에게 제공하는 경우 누구에게, 어떤 이유로, 무엇을 제공하며, 언제까지 이용하게 되는지를 이용자에게 알리고 동의를 획득해야 한다.

※ 관련근거 : 정보통신망법 제24의2(개인정보의 제공 동의 등)

Tip

〈제3자 제공이란?〉

사업자가 수집한 개인정보를 자신의 업무와는 관계없는 제3자에게 제공하는 것

- 예 : 대형할인마트에서 고객정보를 보험사(보험영업)에 제공, 정유사 회원정보를 소핑업체의 상품이나 서비스 홍보를 위해 제공 등

예시화면

개인정보를 제공하는 자	제공받는 자의 개인정보 이용목적
ooo 개인사	신규 서비스의 소개 (매달발송)
ooo 소핑몰	제휴카드 홍보 (월레미캐팅)

제공하는 개인정보의 항목	제공받는 자의 개인정보 보유 및 이용기간
성명, 이메일 주소	제공한날로부터 3개월 후 삭제
성명, 이메일 주소	제공한날로부터 3개월 후 삭제

동의함

동의안함

예시화면과 같이 다음 4가지 항목을 알리고 동의를 획득해야 한다.

- ① 개인정보를 제공받는 자
- ② 제공받는 자의 개인정보 이용목적
- ③ 제공하는 개인정보 항목
- ④ 제공받는 자의 개인정보 보유 및 이용기간

알고가기

개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공할 경우, 이용약관에 명시된 사항 외에 ①개인위치정보를 제공받는 제3자와 ②제공목적은 개인위치정보주체에게 고지하고 동의받아야 한다. 위치기반서비스사업자는 이용자에게 제3자 제공에 대한 동의를 획득한 후에도, 제3자에게 개인위치정보를 제공하는 경우 매회 ①개인위치정보를 제공하는 제3자, ②제공일시, ③제공목적은 이용자에게 즉시 통보해야 한다.

예시화면



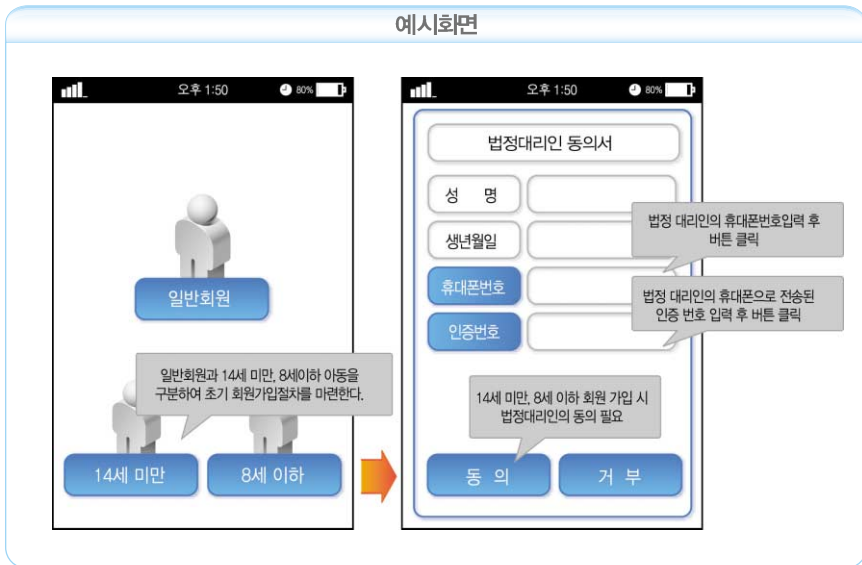
6 미성년자 개인정보 수집시 법정대리인 동의 획득하기

만 14세 미만의 아동의 개인정보 및 개인위치정보를 수집·이용·제공하기 위해서는 법정대리인으로부터 동의를 획득해야 한다.

※ 관련근거 : 정보통신망법 제31조(법정대리인의 권리)

위치정보보호법 제25조(법정대리인의 권리)

위치정보보호법 제26조(8세 이하의 아동 등의 보호를 위한 위치정보 이용)



법정대리인의 동의를 얻기 위한 방법은 다음과 같다.

- ① 일반 회원과 만 14세 미만 아동의 가입경로를 별도로 구분한다.
- ② 아동에게 법정대리인의 성명, 연락처, 이메일 등의 정보를 수집하여 법정대리인에게 동의 여부를 문의한다.
- ③ 법정대리인으로부터 동의한다는 내용의 회신을 받으면 아동이 서비스를 이용할 수 있도록 한다.



〈8세 이하 아동 등의 위치정보 이용〉

8세 이하 아동 등은 법정대리인(보호의무자)이 개인위치정보의 수집·이용·제공에 동의하는 경우 본인의 동의가 있는 것으로 본다.

7 주민등록번호의 사용 제한

정보통신서비스 제공자는 원칙적으로 주민등록번호를 수집·이용할 수 없다. 다만 법에 따라 본인확인기관으로 지정 받은 경우, 다른 법령에서 규정한 경우, 그리고 방송통신위원회가 고시한 경우에는 주민등록번호를 수집·이용할 수 있다. 주민등록번호 수집·이용이 허용된 경우에도 본인확인을 할 수 있는 대체수단을 제공해야 한다.

※ 대체수단(예) : i-PIN 인증(본인확인기관에서 발급받아 본인확인을 할 수 있는 서비스) 등

※ 관련근거 : 정보통신망법 제23조의2(주민등록번호의 사용 제한)



〈주민등록번호를 수집하도록 규정한 다른 법률(예)〉

- 금융실명거래법 제3조
- 전자서명법 제15조
- 전자금융거래법 제16조
- 부가가치세법 제16조, 제17조의2, 제33조
- 소득세법 제145조, 164조

8 개인정보 수집 목적에 한해서만 이용하기

앱 서비스 제공자는 수집한 개인정보 및 개인위치정보를 이용자로부터 동의받은 목적의 범위에서만 이용해야 한다.

※ 관련근거 : 정보통신망법 제24조(개인정보의 이용 제한)

위치정보보호법 제21조(개인위치정보 등의 이용·제공의 제한 등)

신규 서비스 도입 등으로 개인정보를 추가적으로 수집하거나 이용 범위가 변경되는 경우에는 이용자에게 동의를 다시 획득해야 한다.



〈앱 개발 시 주의사항〉

- ① 앱 개발자는 서비스 제공자가 개인정보 수집 목적과는 다른 목적(상업적, 개인적 등)으로 개인정보를 활용하기 위한 어떠한 기능도 제공해서는 안된다.
- ② 웹 회원을 보유하고 있는 앱의 경우, 앱에서 추가적으로 수집하는 개인정보가 있다면 이용자에게 추가적인 동의를 획득해야 한다.
- ③ 위치정보 수집·이용·제공 등과 관련하여 위치정보 이용약관이 변경될 경우 방송통신위원회에 변경신고해야 한다.

9 회원정보 열람·정정 등 이용자 권리 보장하기

개인정보 및 개인위치정보를 수집·이용·제공하는 경우에는 이용자가 동의철회, 일시중지, 열람·정정할 수 있는 기능을 제공해야 하고, 이용자 요구에 대해 지체 없이 적절한 조치를 취해야 한다.

※ 관련근거 : 정보통신망법 제30조(이용자의 권리 등)

위치정보보호법 제24조(개인위치정보주체의 권리 등)

앱 개발자는 예시화면과 같이 이용자 스스로 자신의 개인정보 상태를 확인하고 동의 철회, 열람·정정 등이 가능하도록 기능을 구현해야 한다.



10 개인정보 즉시 파기하기

개인정보의 수집 목적 달성 및 이용기간의 종료, 또는 폐업하는 경우에는 보유하고 있는 개인정보를 지체 없이 파기해야 한다.(이벤트 광고 목적으로 개인정보 수집 후 이벤트 종료시, 회원탈퇴시 등) 개인위치정보 또한 수집·이용·제공 목적을 달성한 때에는 위치정보보호법 제16조에 따라 기록·보존해야 하는 위치정보 수집·이용·제공사실 확인자료 외의 개인위치정보는 즉시 파기하여야 한다.

※ 관련근거 : 정보통신방법 제29조(개인정보의 파기)
 위치정보보호법 제23조(개인위치정보의 파기 등)



〈지체 없이 파기란?〉

합리적 이유 및 근거가 없는 한 즉시 파기하는 것을 의미한다. 다만, 타 법률에따라 개인정보를 보존하여야 하는 경우는 해당되지 않는다.

예시화면

회원 탈퇴 및 동의 철회

> 수집된 개인정보 내역

개인정보 동의범위	동의철회
수집정보 : 성명, 이메일주소, 휴대전화번호 수집·공시사항, 상품소개 개인정보 보유 및 이용기간 : 회원탈퇴 시 삭제	동의철회 (회원탈퇴)

> 연락처 ☎ 02-000-0000 ✉ admin@kbsa.co.kr

> 회원탈퇴 시

즉시 파기되는 개인정보

이름과 전화번호를 제외한 모든 개인정보 [이메일, 패스워드, 주소, 이메일주소는 회원 탈퇴 즉시 본사의 모든 시스템에서 파기됩니다.]

일정기간 보유되는 개인정보

통신비밀보호법 제 15조의 2통신사실 확인자료 제출의무에 의거 하여 다음과 같은 개인정보는 12개월간 보관 후 파기됩니다.
-이름, 전화번호

앱 개발자는 ①개인정보의 수집 및 이용 목적을 달성하거나 ②이용자에게 동의를 획득한 개인정보 보유 및 이용기간이 종료된 경우 ③폐업하는 경우에는 보유하고 있는 개인정보를 지체 없이 파기하도록 구현해야 한다.

다만, 예시화면과 같이 다른 법률 규정 등에 따라 개인정보를 보유해야 하는 합리적인 이유와 근거가 있으면 해당 기간 내에 개인정보를 보유할 수 있다.

개인정보를 파기할 때에는 재생할 수 없도록 파기해야 한다. 종이 출력물의 경우 분쇄기로 분쇄하거나 소각해야 하며 컴퓨터 파일 형태로 저장된 개인정보 기록은 ‘로우레벨포맷’이나, ‘일반포맷’을 한 뒤 불필요한 정보를 여러번 덮어 씌우는 방법으로 다시는 재생할 수 없도록 조치해야 한다.

11 기술적 보호조치 구현하기

개인정보에 불법적인 접근 및 안전한 저장·전송을 위하여 암호화 기술 및 접근통제 설비 등을 운영해야 한다.

※ 관련근거: 정보통신망법 제28조(개인정보의 보호조치)

위치정보보호법 제16조(위치정보의 보호조치 등)



개인정보 및 위치정보의 기술적·보호조치에 관한 자세한 사항은 ‘한국인터넷진흥원 홈페이지(www.kisa.or.kr)»자료실‘ 참조

- 개인정보의 기술적·관리적 보호조치 기준 및 해설서
- 위치정보보호를 위한 관리적·기술적 보호조치 권고 및 해설서

예시화면

앱 개발자는 예시화면과 같이 이용자가 안전한 비밀번호를 이용할 수 있도록 ① 비밀번호 작성규칙을 수립하고, 이행해야 한다.

주민번호, 계좌번호, 신용카드번호, 패스워드 등 중요 정보를 화면에 표시할 때는 ②리마킹 처리하도록 한다.

개인정보 및 개인위치정보를 전송, 서버 및 단말기에 저장시 ③암호화하도록 한다.

또한, 네트워크 보안 및 접근통제 등을 위해 ④방화벽 등 정보보호 시스템 설치·운영, ⑤개인정보 및 개인위치정보에 접근한 기록보존·백업, ⑥악성프로그램 방지를 위한 백신 프로그램 설치 등을 해야한다.

알고가기

위치정보사업자들은 위치정보 수집·이용 등의 사실 확인자료를 위치정보시스템에 자동으로 기록·보존하고, 누출·변조·훼손되지 않도록 기술적 조치를 취해야 한다.

〈위치정보 수집 사실 확인자료(예시) : 위치정보사업자〉

※ 2006. 11. 15 14:30분에 B사업자의 요청으로 A통신사업자가 Cell-ID방식으로 C이용자의 위치정보를 수집

수집자	요청서비스	요청자	수집방법	수집요청시간	수집종료시간
A사업자	친구찾기	B사업자	Cell-ID	2006.11.15.14:30	2006.11.15.14:35

〈위치정보 이용·제공 사실 확인자료(예시) : 위치기반서비스사업자〉

※ B사업자는 A사업자로부터 수집한 정보를 C이용자에게 14:30~35분까지 SMS/E-mail으로 정보를 제공

취득경로	제공서비스	제공받는자	제공시간	제공방법
A사업자	친구찾기	C이용자	2006.11.15.14:30~35	SMS/E-mail등



참고자료



1. 관련법령(법률, 고시, 해설서 등)

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률(www.kcc.go.kr»법령정보)
- 위치정보의 보호 및 이용 등에 관한 법률(www.kcc.go.kr»법령정보)
- 정보통신서비스제공자를 위한 개인정보보호 가이드(privacy.kisa.or.kr)»자료실
- 위치정보의 보호 및 이용 등에 관한 법률 해설서(www.kisa.or.kr»자료실)
- 개인정보의 기술적·관리적 보호조치 기준 및 해설서(www.kisa.or.kr»자료실)
- 위치정보보호를 위한 관리적·기술적 보호조치 권고 및 해설서(www.kisa.or.kr»자료실)
- 위치정보 관련 사업 허가·신고 양식(www.kcc.go.kr)»정책/정보센터»자료마당»사업자 제출자료)

2. 앱 개발관련

- 스마트 모바일 앱 개발 지원센터(www.smac.or.kr)
- SKT(dev.tstore.co.kr)
- KT(seller.ollehmarket.com)
- LG U+(devpartner.lguplus.co.kr)
- 구글(developer.android.com)
- 애플(developer.apple.com)

3. Secure Coding 관련

- 정보시스템 SW 개발보안 가이드(www.mopas.go.kr»정책자료»참고자료실)
- The CERT Oracle Secure Coding Standard for Java(www.cert.org)
- The CERT C Secure Coding Standard(www.cert.org)
- The CERT C++ Secure Coding Standard(www.cert.org)
- iOS Secure Coding Guide(developer.apple.com)

4. 개인정보보호 조치 안내서

- 보안서버 구축안내서(www.kisa.or.kr»자료실)
- 패스워드선택 및 이용안내서(www.kisa.or.kr»자료실)
- 암호이용 안내서(www.kisa.or.kr»자료실)
- 암호이용 구현 안내서(seed.kisa.or.kr»자료실)
- 암호알고리즘 및 키길이 이용 안내서(www.kisa.or.kr»자료실)
- 무선랜 보안 안내서(www.kisa.or.kr»자료실)
- 와이브로 보안기술 안내서(www.kisa.or.kr»자료실)
- 아이핀 도입 안내서(www.kisa.or.kr»자료실)
- 웹사이트 개발 · 운영을 위한 개인정보 안내서(www.kisa.or.kr»자료실)

5. 개인정보보호 관련 정보제공 홈페이지

- 개인정보보호 포털 및 위치정보보호(www.i-privacy.kr)
- 웹사이트 개인정보 보호조치 안내(guide.kisa.or.kr)
- 아이핀(i-pin.kisa.or.kr)
- 개인정보보호 자가진단(www.privacycheck.or.kr)
- 개인정보침해신고센터(privacy.kisa.or.kr)
- 보안서버(secsv.kisa.or.kr)
- 암호이용(seed.kisa.or.kr)

앱 개발자를 위한
개인정보보호
안내서

