

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

개인정보보호 가이드

2019년 08월 27일



정보보안센터

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

개정 이력

개정번호	변경내용	작성자	작성일
1.0	최초작성	정보보안팀 남선미	2012.11.02
1.1	숨김처리(마스킹) 기준 일부 변경	정보보안 강화 TF 남선미	2014.04.18
1.2	숨김처리(마스킹) 기준 일부 변경	정보보안 강화 TF 남선미	2014.04.22
1.3	운전면허번호 숨김처리(마스킹) 기준 추가	정보보안 강화 TF 남선미	2014.04.22
1.4	이름 마스킹 기준 설명 추가	정보보안 강화 TF 남선미	2014.04.25
1.5	문서제목 변경 미준수 시 벌칙(법규, 고시)현행화	보안이행팀 권혜선	2015.06.19
1.6	정보통신망법[시행2016.9.23] 개정 및 관련 고시 내용 반영, 개인정보보호법 개정[시행2016.9.30] 반영	보안정책팀 김재원	2016.07.06
1.7	개인정보 안전성 확보조치 기준[시행2019.06.07] 반영 미준수 시 벌칙(법규, 고시)현행화	보안정책팀 이민지	2019.08.27

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

목 차

1. 개인정보처리방침	4
준수 기준	4
관련 근거	4
미준수 시 벌칙	4
보호 조치	4
미준수 예시	6
2. 개인정보 암호화	8
준수 기준	8
관련 근거	8
미준수 시 벌칙	8
보호 조치	9
미준수 예시	11
3. 개인정보 수집·이용, 제공·위탁에 대한 동의	16
준수 기준	16
관련 근거	16
미준수 시 벌칙	16
보호 조치	17
미준수 예시	19
4. 주민등록번호 수집·이용 제한	23
준수 기준	23
관련 근거	23
미준수 시 벌칙	23
보호 조치	23
미준수 예시	24
5. 개인정보 접속기록 저장 및 보관	26
준수 기준	26
관련 근거	26
미준수 시 벌칙	26
보호 조치	26
미준수 예시	27
6. 개인정보 숨김처리	28
준수 기준	28
관련 근거	28
보호 조치	28
미준수 예시	29

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

1. 개인정보처리방침

준수 기준	정보통신서비스 제공자 등은 이용자의 개인정보를 처리하는 경우에는 개인정보 처리방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
관련 근거	<ul style="list-style-type: none"> 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법") 제 27 조의 2 (개인정보처리방침의 공개) 및 시행령 제 14 조(개인정보처리방침의 공개 방법 등) 개인정보보호법 제 30 조(개인정보 처리방침의 수립 및 공개)
미준수 시 벌칙	<ul style="list-style-type: none"> 정보통신망법 - 개인정보 처리방침을 공개하지 아니한 경우 : 2천만원 이하의 과태료 개인정보보호법 - 개인정보 처리방침을 정하지 아니하거나 공개하지 아니한 경우 : 1천만원 이하의 과태료

정보통신서비스제공자 등이 이용자의 개인정보를 처리하는 경우, 개인정보처리방침을 정하고 이를 이용자가 언제든지 쉽게 확인할 수 있도록 공개하도록 하고 있다.

이용자의 개인정보 처리에 대한 회사의 방침을 마련하고 이를 이용자가 언제든지 쉽게 확인할 수 있도록 공개해야 한다.

인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 이용자가 쉽게 알아볼 수 있도록 글자 크기, 색상 등을 활용하여 개인정보처리방침을 쉽게 확인할 수 있도록 표시하여야 한다.

개인정보처리방침을 변경하는 경우에는 그 이유 및 변경내용을 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다. (공지방법 : 인터넷 홈페이지 첫 화면의 공지사항 란 또는 별도의 창을 통하여 공지하거나 이메일 등으로 공지, 점포 사무소 안에 비치해야 함)

보호 조치

(1) 개인정보처리방침의 공개방법

웹사이트 첫 화면에 '개인정보처리방침' 제목을 게시하고, 클릭하면 세부 내용이 보여지도록 페이지를 연결하면 된다. 단, 주의하여야 할 것은 명칭을 반드시 '개인정보처리방침'으로 하여야 한다.

※ 반드시 "개인정보 처리방침"이라는 명칭을 사용하고, 글자크기, 색상 등을 활용하여 다른 고지사항(이용약관, 저작권 안내 등)과 구분하여 정보주체가 쉽게 확인하도록 해야 함



개인정보처리방침

찾아오시는 길 | 고객센터 | RSS | KISA | Twitter | NAVER 블로그 | 해킹·스캠·개인정보침해 신고는 118

본원 (05717) 서울시 송파구 중대로 135 (가락동 78) IT벤처타워 Tel. 02-405-5118 / Fax. 02-405-5119

본 홈페이지에 게시된 이메일 주소가 자동 수집되는 것을 거부하며, 이를 위반시 정보통신망법에 의해 처벌됨을 유념하시기 바랍니다.

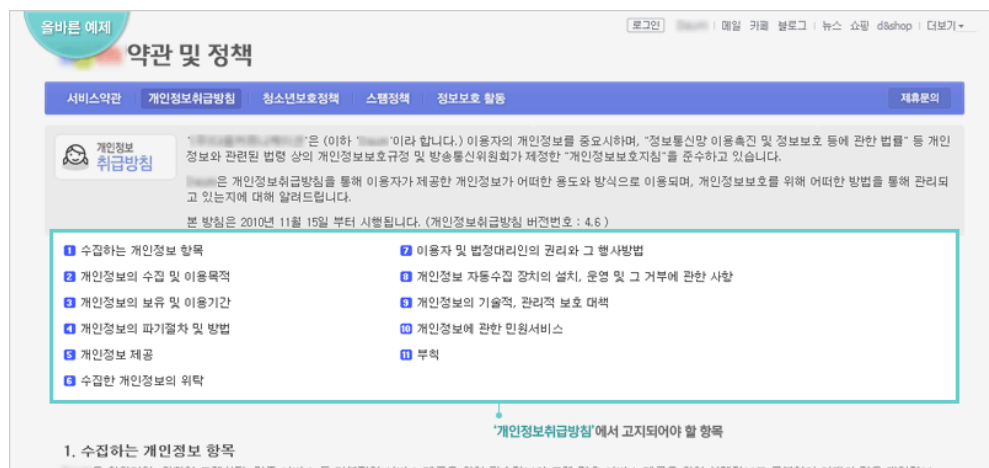


문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

(2) 개인정보처리방침에 반드시 포함되어야 하는 사항

개인정보처리방침에는 아래의 내용이 빠짐 없이 포함되어야 하며, 그 외 내부 방침이 있는 경우 추가할 수 있다.

- 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법
- 개인정보를 제 3 자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭), 제공받는 자의 이용 목적과 개인정보의 항목(해당하는 경우)
- 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법
- 개인정보 처리위탁을 하는 경우 위탁 업무의 내용 및 수탁자(해당하는 경우)
- 이용자 및 법정대리인의 권리와 그 행사방법
- 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
- 개인정보 보호책임자의 성명 또는 개인정보보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처



(3) 개인정보처리방침 작성 가이드

개인정보처리방침 작성 예시를 참고하여 작성하되, 운영하는 웹사이트 내용에 맞게끔 내용을 수정 반영하여야 하며, 필수 7 가지 고지 항목이 모두 들어가야 한다.

- 작성 예시
 - KT 시스템의 경우 KT 홈페이지 또는 올레닷컴 사이트의 개인정보처리방침 참고
 - 기타: 개인정보보호 종합포털 참고

https://www.privacy.go.kr/inf/gdl/selectBoardArticle.do?nttlId=1767&bbsId=BBSMSTR_000000000044&bbsTyCode=BBST01&bbsAttrbCode=BBSA03&authFlag=Y&pageIndex=1&searchCnd=&searchWrd=&replyLc=0

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

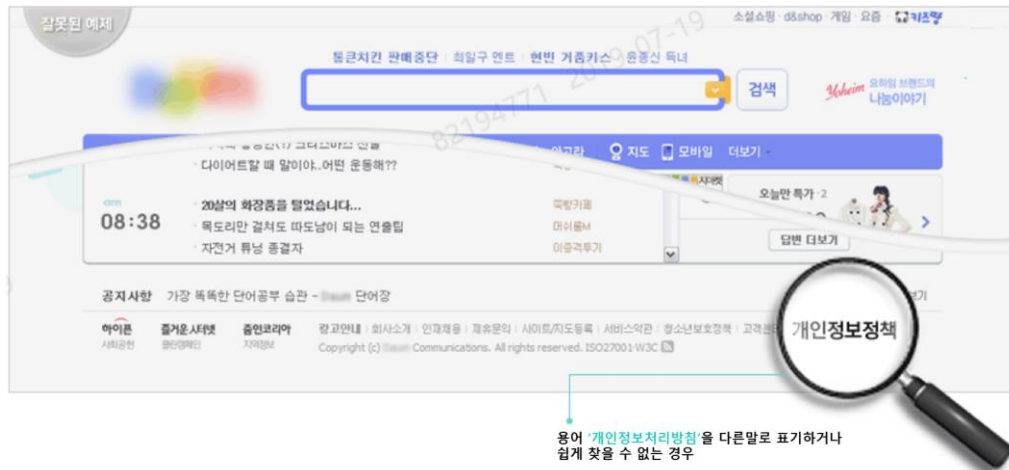
(4) 개인정보처리방침 현황 관리

개인정보처리방침의 내용 변경이 발생할 경우 현행 관리를 하여야 하고, 개인정보처리방침에 따라 웹사이트 등이 구현되어야 하며, 이를 준수하여야 한다.

미준수 예시

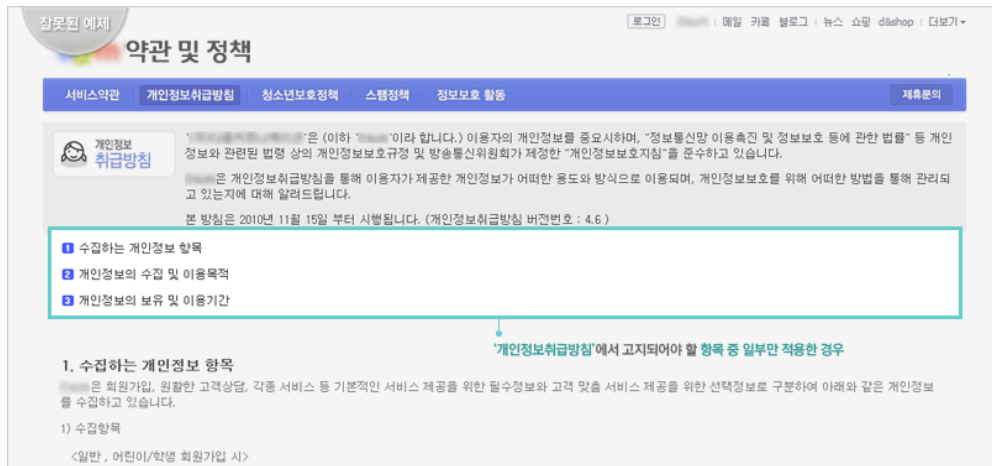
(1) [예시1] '개인정보처리방침' 명칭 오류

'개인정보처리방침'을 다른 말(예. '개인정보보호정책', '개인정보취급방침' 등)로 표기한 경우



(2) [예시2] '개인정보처리방침'에서 고지되어야 할 항목 누락

'개인정보처리방침'에서 고지되어야 할 항목 중 일부만 적용한 경우



(3) [예시3] '개인정보처리방침'과 실제 구현 내용 상이

- '개인정보처리방침'에서 고지되어 있는 내용과 실제 수집, 또는 구현되어 있는 내용이 다른 경우
- '개인정보처리방침'에는 처리위탁/제3자 제공 내용이 포함되어 있으나, 회원가입 시 동의에는 포함되어 있지 않은 경우 등

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

[회원가입 시 필수정보 : 이름, 이메일, 비밀번호, 주소, 일반전화, 휴대전화]

[처리방침 내 필수정보 : 이름, 이메일, 비밀번호]

(4) [예시4] '개인정보처리방침' 내용 현행관리 안됨

'개인정보처리방침' 내용에 변경이 발생한 경우 현행관리가 되지 않는 경우

(예. 개인정보보호책임자 미 현행화, 개인정보 위탁, 제3자 제공 업체 미 현행화 등)

점검 방법

- (1) 홈페이지 첫 화면에 '개인정보처리방침'이 게시되어 있는지 확인한다.
- (2) '개인정보처리방침'에 포함되어야 하는 사항이 모두 포함되어 있는지 확인한다.
- (3) '개인정보처리방침' 내용과 실제 구현된 내용 또는 준수하고 있는지 확인한다.
- (4) '개인정보처리방침' 내용이 현행 관리되는지 확인한다.
- (5) '개인정보처리방침'이 변경된 경우 변경내용을 공지했는지 확인한다.

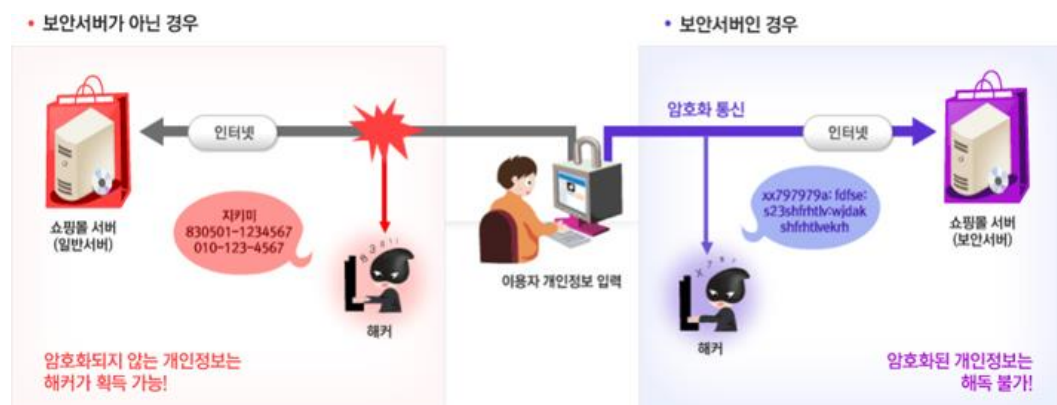
문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

2. 개인정보 암호화

준수 기준	<p>정보통신서비스 제공자 등은 개인정보가 안전하게 저장·전송될 수 있도록 암호화 하여야 한다.</p> <p>- 암호화 대상 : 고유식별정보, 금융정보, 비밀번호, 바이오정보, 위치정보</p>
관련 근거	<ul style="list-style-type: none"> 정보통신망법 제 28 조(개인정보의 보호조치) 및 시행령 제 15 조(개인정보의 보호조치) 개인정보보호법 제 29 조(안전조치 의무) 및 시행령 제 30 조(개인정보의 안전성 확보 조치) 개인정보의 기술적·관리적 보호조치 기준 제 6 조(개인정보의 암호화) 개인정보의 안전성 확보조치 기준 제 7 조(개인정보의 암호화)
미준수 시 벌칙	<ul style="list-style-type: none"> 정보통신망법 - 암호화 조치를 하지 아니한 경우 : 3 천만원 이하의 과태료 정보통신망법 - 암호화 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우 : 2 년 이하의 징역 또는 2 천만원 이하의 벌금(회사 : 위반행위와 관련한 매출액의 100 분의 3 이하에 해당하는 과징금) 개인정보보호법 - 안전성 확보에 필요한 조치를 하지 않은 경우 : 3 천만원 이하의 과태료 개인정보보호법 - 안전성 확보에 필요한 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우 : 2 년 이하의 징역 또는 2 천만원 이하의 벌금

정보통신서비스 제공자 등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

- 비밀번호의 일방향 암호화 저장
- 고유식별정보 및 금융정보(신용카드번호, 계좌번호), 바이오정보 등의 암호화 저장
- 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송·수신하는 경우, 보안서버 구축 등의 조치
- 그 밖에 암호화 기술을 이용한 보안조치



문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

보호 조치

(1) 암호화 대상

- 인증 정보 : 비밀번호
- 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
- 금융정보 : 계좌번호, 신용카드번호
- 위치정보
- 바이오정보

데이터 암호화 대상(DB, 파일, 백업매체 등)

정보구분	정보명	정보통신방법	개인정보 보호법	위치정보 보호법	적용암호화 방식
인증정보	비밀번호	○	○	○	일방향 암호(해쉬암호) - 알고리즘 : SHA-256 이상 ※ 유출 대비 SALT 추가 권고 ※ SHA-1 은 사용불가
	바이오정보	○	○		
고유식별정보	주민등록번호	○	○		양방향 암호(블록암호) - 알고리즘 : 보안강도 128bit 이상의 AES, ARIA, SEED - 모드 : CBC 권고 ※ 주민번호는 뒤 6 자리만 별도저장 시에도 해당정보 암호화 필수
	여권번호	○	○		
	운전면허번호	○	○		
	외국인등록번호	○	○		
금융정보	계좌번호	○			
	신용카드번호	○			
위치정보	위치정보			○	

(2) 암호화 방식 및 사용 알고리즘

개인정보 및 인증정보는 다음과 같이 암호화하여 저장하여야 한다.

대상	암호화 방식	권고하는 알고리즘
인증정보(비밀번호)	일방향 암호화	SHA-256 이상 적용 (MD5, SHA-1 등 사용 금지)
고유식별정보 금융정보 바이오정보, 위치정보	양방향 암호화	SEED, AES-128 이상 적용

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

[참고] 안전한 암호 알고리즘

구분	알고리즘 명칭
대칭키 암호 알고리즘	SEED ARIA-128/192/256 AES-128/192/256 Blowfish Camelia-128/192/256 MISTY1 KASUMI 등
공개키 암호 알고리즘	RSA KCDSA(전자서명용) RSAES-OAEP RSAES-PKCS1 등
일방향 암호 알고리즘	SHA-224/256/384/512 Whirlpool 등

(3) 구간별 암호화 방법

개인정보는 서버 및 PC 등 저장 시 암호화하여 저장하여야 하며, 전송구간에서도 암호화 통신을 해야 한다.

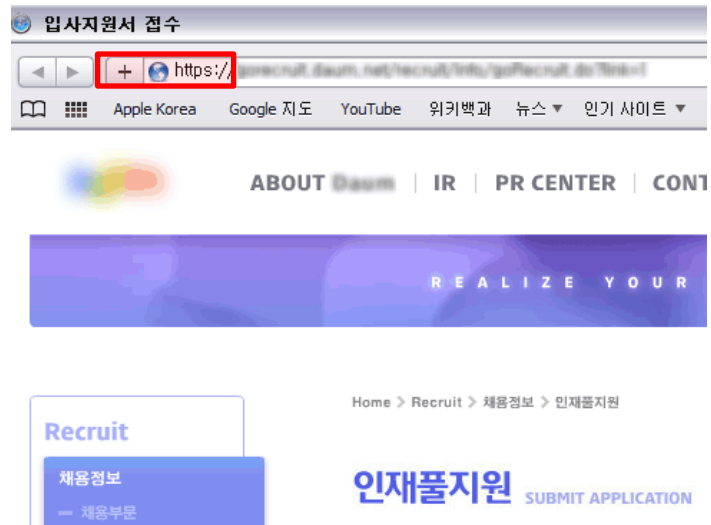
PC 에 저장할 경우에는 DRM 등으로 암호화하여 저장하여야 하며, 서버에 저장할 경우 DB, 파일에 대해서 전용 암호화 솔루션을 사용하거나, '안전한 암호 알고리즘'을 이용하여 암호화하여 한다.

개인정보 전송 시 암호화는 SSL 을 적용하거나, 별도의 응용프로그램을 이용하여 송수신시 암호화 적용 후 전송해야 한다.

구분		암호화 여부	암호화 방법
저장	서버	○	전용 암호솔루션 적용 또는 안전한 암호 알고리즘 이용한 암호화
	PC	○	DRM 또는 파일에 암호 설정
전송	PC <-> 서버	○	SSL 또는 별도 보안 응용프로그램 적용
	개인정보취급자 간 (PC <-> PC)	○	암호화된 파일 첨부
	개인정보처리시스템 간 (서버 <-> 서버)	○	외부 시스템과 연동하는 경우에는 전용회선 또는 VPN 이용하거나

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

[SSL을 적용한 경우]



[별도 응용프로그램을 적용한 경우]



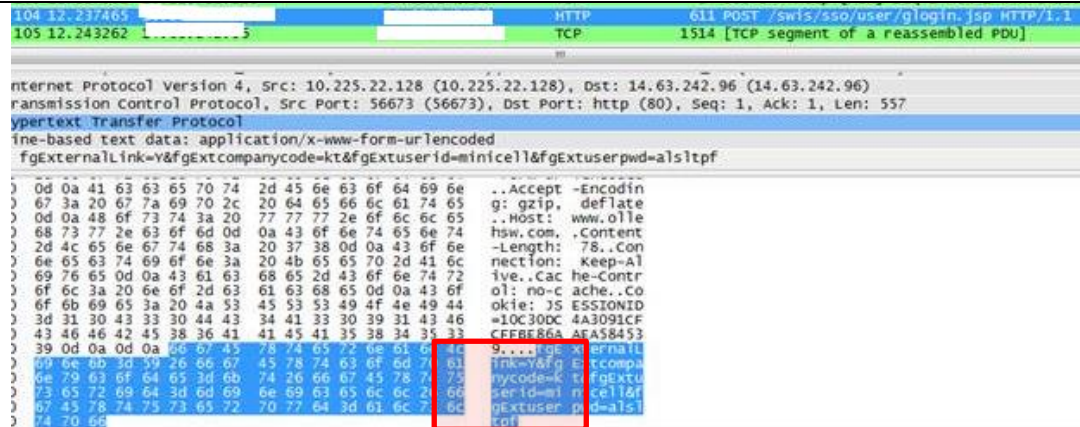
※ 암호화에 대한 상세 내용은 '개인정보 암호화 매뉴얼-KT' 또는 '개인정보 암호화 조치 안내서-KISA' 참고

미준수 예시

(1) [예시1] 비밀번호를 암호화하지 않고 전송

비밀번호를 암호화하여 전송하지 않고 평문으로 전송하는 경우
(내부망에서도 암호화하여 전송해야 함)

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7



(2) [예시2] 비밀번호를 평문으로 저장하거나 단순 encoding만 적용

비밀번호는 SHA-256 등 일방향 암호화하지 않고 평문으로 저장하거나, base64 encoding만 적용하여 저장하는 경우

[비밀번호 평문 저장]

EMP_NO	NAME	PASSWORD	EMAIL
92: [redacted]	김영민	hs [redacted]	hanki
92: [redacted]	조영민	67 [redacted]	joym
92: [redacted]	김영민	66 [redacted]	kimy
92: [redacted]	한영민	ha [redacted]	hany
92: [redacted]	성영민	12 [redacted]	seoy
92: [redacted]	서영민	14 [redacted]	seoy
92: [redacted]	남영민	66 [redacted]	namy
92: [redacted]	이영민	53 [redacted]	ioy
92: [redacted]	송영민	djs [redacted]	soy
92: [redacted]	한영민	ha [redacted]	hany

(3) [예시3] 비밀번호를 양방향 암호화 하여 저장

비밀번호는 당사자 이외에는 확인이 불가하도록 일방향 암호화 저장해야 하나, 양방향 암호화(예. AES-128 등)를 적용하여 저장한 경우 (양방향 암호화는 복호화 가능하므로 다른 사람이 비밀번호를 확인할 수 있으므로 문제가 됨)

[비밀번호 양방향 암호화 적용]

USER_ID	USER_NAME	PASSWORD	DEPART
963	이영민	HcnJf [redacted]	총무팀
200	이영민	8GaC [redacted]	홍보팀
857	서영민	4FxW [redacted]	홍보팀
200	윤영민	ihLT8 [redacted]	홍보팀
972	이영민	Y50V [redacted]	CR부서
200	이영민	Y50V [redacted]	개인교과
903	임영민	COB [redacted]	중부팀
866	임영민	COB [redacted]	전북팀
912	임영민	COB [redacted]	강남팀
880	김영민	COB [redacted]	제주팀

(4) [예시4] 비밀번호가 마스킹 처리되지 않고 평문으로 웹화면에 노출

비밀번호가 마스킹 처리 등을 하지 않고 웹 페이지에 그대로 노출되는 경우

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

(7) [예시7] 안전하지 않은 암호 알고리즘을 이용하여 주민등록번호 등을 암호화하여 저장
 안전하지 않은 암호 알고리즘(예. DES 등)으로 고유식별정보와 금융정보를 암호화하여 저장하는 경우

SEX_DISTINCTION	SEARCH_FLAG	TITLE_NM	SOCIAL_NO
남	Y	사원	RXSJGNIIM2JouD4+jhM5/qQ==
남	Y	사원	nPgZ7IQCgrZbrYU/yO+sNw==
남	Y	사원	qpg3fUkVg1BZ3Ld3NREA==
남	Y	과장	PKDYHj9an2NUGfEJS2YJCw==
남	Y	사원	MfBaSS11rUt0OnmqXZROQ==
남	Y	사원	gfVbDFZr8XdqeXNpM8N7rg==
남	Y	사원	UNjurFy323zdHvYOL829Q==
남	Y	사원	6khaYpY8W1xHoxJ+FrBnkg==
남	Y	과장	kVDrFPpGGGmLyul28tt/Kg==

■ 회원정보조회

회원ID 또는 주민등록번호 또는 E-Mail을 입력하세요.

◇ 회원 ID	<input type="text"/>
◇ 주민번호	<input type="text"/> (YYMMDD-xxxxxx)
◇ E-Mail	<input type="text"/> (userid@kt.co.kr)
◇ 사용자명	<input type="text"/>

점검 방법

- (1) 비밀번호 및 고유식별정보, 금융정보를 처리하는 페이지가 있는지 확인한다.**
 - (예) 로그인 페이지, 회원가입 페이지, 비밀번호 수정 페이지, 회원정보 수정 페이지, 비회원으로 게시판 글쓰기 등 비밀번호 입력 페이지 등
- (2) 비밀번호 및 고유식별정보, 금융정보를 처리하는 웹페이지에서 SSL 또는 별도 암호프로그램이 적용되어 있는지 확인한다.**
 - 세부 확인 사항은 아래 '상세 점검 방법' 참고
- (3) 웹화면, 소스 등에 불필요한 정보가 노출되지 않는지 확인한다.**
- (4) 비밀번호 및 고유식별정보, 금융정보 저장 시 안전한 암호 알고리즘을 적용하여 암호화되어 있는지 확인한다.**

[상세 점검 방법]

■ 전송구간 암호화 여부 확인

- 로그인 시 ID/PW가 암호화되어 전송되는지 확인한다.
 - 방법 : Wireshark를 이용하여 로그인 단계에서 패킷을 캡처하여 PW가 암호화 되었는지 확인
- 비밀번호 수정, 회원정보 수정 등의 페이지에서 개인정보가 암호화되어 전송되는지 확인한다.

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

3. 개인정보 수집·이용, 제공·위탁에 대한 동의

준수 기준	<p>개인정보를 수집·이용할 때는 사전에 이용자로부터 동의를 받아야 하고, 수집한 개인정보를 제3자에게 제공하거나 개인정보 처리 업무를 위탁하는 경우에도 사전에 이용자의 동의를 받아야 한다.</p> <p>수집·이용, 제공, 위탁에 대한 동의는 별도로 받아야 하며, 수집·이용에 대한 동의는 필수, 제공·위탁에 대한 동의는 선택 동의로 구현되어야 한다. 선택적 동의 항목에 대해 동의하지 않았다고 해서 서비스 가입이 불가해서는 아니 된다.</p> <p>개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 관련 사항(개인정보의 수집 출처, 개인정보의 처리 목적 등)을 정보주체에게 알려야 한다.</p>
관련 근거	<ul style="list-style-type: none"> 정보통신망법 제 22 조(개인정보의 수집·이용 동의 등), 제 24 조의 2(개인정보의 제공 동의 등), 제 25 조(개인정보의 처리위탁), 제 26 조의 2(동의를 받는 방법) 및 시행령 제 12 조(동의획득방법) 개인정보보호법 제 15 조(개인정보의 수집·이용), 제 17 조(개인정보의 제공), 제 18 조(개인정보의 이용·제공 제한), 제 20 조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지), 제 22 조(동의를 받는 방법)
미준수 시 벌칙	<ul style="list-style-type: none"> 정보통신망법 - 이용자의 동의를 받지 아니하고 개인정보를 수집, 이용, 제공하는 경우 : 5 년 이하의 징역 또는 5 천만원 이하의 벌금(회사 : 위반행위와 관련한 매출액의 100 분의 3 이하에 해당하는 과징금 부과) 정보통신망법 - 이용자의 동의를 받지 아니하고 이용자의 개인정보를 국외에 처리위탁·보관한 경우 : 2 천만원 이하의 과태료(회사 : 위반행위와 관련한 매출액의 100 분의 3 이하에 해당하는 과징금 부과) 외에 개인정보보호법에서는 개인정보 수집 및 선택동의에 대한 서비스 제공 거부 등에 대하여 3 천만원 이하의 과태료를 부과함
<p>개인정보를 이용하려고 수집하는 경우 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다.</p> <ul style="list-style-type: none"> - 개인정보의 수집이용 목적 - 수집하는 개인정보의 항목 - 개인정보의 보유·이용 기간 - 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 (개인정보보호법의 '개인정보처리방침'에 추가된 항목) <p>회원이 가입 등의 상시 서비스 제공 외에 이벤트 등 일시적인 서비스 제공을 위한 개인정보 수집 시에도 동의는 반드시 받아야 한다.</p>	

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

개인정보의 수집·이용, 제공·위탁에 대해 항목별로 별도 동의를 받아야 하며, 개인정보 수집·이용에 대한 동의는 필수이며 그 외는 항목별로 선택적 동의를 받도록 구현해야 한다.

고유식별정보나 민감정보의 경우 원칙적으로 수집할 수 없으며, 불가피하게 수집해야 하는 경우 다른 항목들과 별도로 동의를 받아야 한다.

[참고] 제3자 제공과 업무 위탁의 차이

■ 제3자 제공

- 타사와의 제휴서비스 등을 통해 수집한 개인정보를 제3자에게 제공하는 경우를 말함
- 개인정보 제3자 제공 예 : 다른 회사와 제휴 이벤트를 위한 고객정보 공유, 통신사가 보험사의 TM을 위해 보험사에 고객정보를 제공하는 경우 등

■ 업무 위탁

- 자사의 서비스를 직접 수행하지 않고 다른 회사 등에 위탁하는 경우를 말함
- 개인정보처리 업무 위탁의 예 : 택배회사에 상품 배송 업무 위탁, 고객 민원 처리 아웃소싱, 요금고지서 및 DM 발송, 서비스AS 아웃소싱 등

■ 개인정보 제3자 제공과 업무 위탁의 차이

- 개인정보의 제공·이용 목적이 자사의 서비스 제공을 위한 것이면 업무 위탁에 해당되고, 제3자의 서비스 제공을 위한 것이면 제3자 제공으로 볼 수 있음

보호 조치

(1) 개인정보 수집·이용에 대한 동의 여부 선택 화면 제공

이용자가 개인정보를 입력하기 전 단계에 동의 사항을 고지하고, 동의 여부를 선택할 수 있도록 '동의함' 또는 '동의안함' 버튼을 구현한다.

- 개인정보 수집 예 : 회원가입, 비회원구매, 견적·상담·게시판, 이벤트 등을 이용하기 위한 연락처 등 기재

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

(2) 개인정보 수집·이용에 대한 동의 항목 고지

반드시 개인정보 수집·이용에 대한 3 가지 항목만 별도로 고지하고 동의를 받아야 한다.

- 개인정보 수집·이용에 대한 3 가지 항목 : 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간
- 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 (개인정보보호법의 '개인정보처리방침'에 추가된 항목)

(3) 개인정보 제3자제공·업무위탁에 대한 동의 여부 선택 화면 제공

수집한 개인정보를 제 3 자에게 제공하거나 개인정보 처리 업무를 위탁 하는 경우에는 사전에 이용자의 동의를 받아야 한다. 수집한 개인정보 제공 전 단계에 동의 사항을 고지하고, 동의 여부를 선택할 수 있도록 '동의함' 또는 '동의안함' 버튼을 구현한다. 단, 서비스 제공에 관한 계약을 이행하기 위해 필요한 업무의 위탁인 경우에는 개인정보처리방침에 게시하면 동의 받지 않아도 된다.

(4) 개인정보 제3자제공·업무위탁에 대한 동의 항목 고지

■ 제3자 제공의 경우

아래 4가지 항목만 고지하고 동의를 받아야 한다.

- 개인정보를 제공받는 자
- 개인정보를 제공받는 자의 개인정보 이용 목적
- 제공하는 개인정보의 항목
- 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

올바른 예제

● 개인정보 제3자 제공 안내

회사는 서비스 향상을 위해서 아래와 같이 개인정보를 제3자와 제휴하고 있으며, 관계 법령에 따라 개인정보를 제3자 제공 시 개인정보를 안전하게 관리할 수 있도록 필요한 사항을 규정하고 있습니다.

회사의 개인정보 제3자 제공 내용은 아래와 같습니다.

- 제공 받는 자 : (주)다음커뮤니케이션
- 개인정보 이용 목적 : 제안 내용의 확인 및 처리
- 제공하는 개인정보 항목 : 이름, 전화번호, E-mail
- 보유 기간 : 제안 채택 시 서비스 반영 시까지, 제안 불채택 시 즉시 파기됨

☐ 위의 '개인정보 제3자 제공'에 동의합니다.

● 개인정보 취급위탁 안내

회사는 서비스 향상을 위해서 아래와 같이 개인정보를 위탁하고 있으며, 관계 법령에 따라 위탁계약 시 개인정보를 안전하게 관리할 수 있도록 필요한 사항을 규정하고 있습니다.

■ 업무 위탁의 경우

아래 2가지 항목만 고지하고 동의를 받아야 한다. 단, 서비스 제공에 관한 계약을 이행하기 위해 필요한 업무의 경우에는 개인정보처리방침에 게시하면 동의 받지 않아도 된다.

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

- 개인정보 처리위탁을 받는 자
- 개인정보 처리위탁을 하는 업무의 내용

(5) 고유식별정보, 민감정보 수집 금지 및 별도 동의

고유식별정보 및 민감정보는 원칙적으로 수집할 수 없으며, 필요한 경우 별도 동의를 받아야 한다.

미준수 예시

(1) [예시1] 개인정보 수집·이용에 대한 동의 화면 미제공

개인정보 수집·이용에 대한 동의 선택 기능이 없는 경우

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

(2) [예시2] '개인정보처리방침' 전체에 대한 동의 화면 제공

개인정보처리방침 전문을 게재하고 개인정보처리방침 전체에 대해 동의를 받거나, 약관에 포함하여 동의를 받는 경우

The screenshot shows a web page with a header section titled '개인정보처리방침 안내' (Personal Information Processing Policy Notice). Below the header, there is a section titled '1. 수집항목' (Collection Items) which lists various personal information items like name, ID, phone number, etc. At the bottom of the page, there is a checkbox labeled '위의 '서비스 이용약관'에 동의합니다.' (I agree to the 'Service Terms of Use' above) and a button labeled '다음단계로' (Next Step).

(3) [예시3] 수집·이용 동의와 제공·위탁 동의 미분리

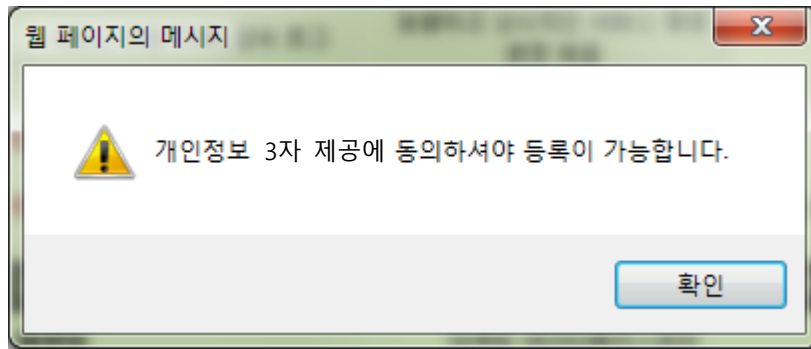
개인정보 수집·이용과 제공·위탁에 대한 동의를 분리하지 않고 하나로 묶어서 일괄적으로 동의를 받는 경우

The screenshot shows a web page with a header section titled '개인정보 수집·이용 안내' (Personal Information Collection and Use Notice). Below the header, there is a section titled '1. 수집항목' (Collection Items) which lists various personal information items. Below this, there is a section titled '2. 개인정보 제3자 제공 안내' (Personal Information Third-Party Provision Notice) which lists various third-party providers. At the bottom of the page, there is a checkbox labeled '위의 '개인정보취급방침' 3가지 항목'에 동의합니다.' (I agree to the 3 items of the 'Personal Information Processing Policy' above) and a button labeled '다음단계로' (Next Step).

(4) [예시4] 제공·위탁에 대해 동의하지 않으면 서비스 가입 불가

- 선택 항목에 대한 동의를 하지 않거나 제공·위탁에 동의하지 않은 경우 회원 가입 등이 불가능한 경우

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7



(5) [예시5] 고유식별정보, 민감정보 수집 시 별도 동의 미적용

고유식별정보나 민감정보를 수집하고 있으나, 이에 대한 별도 동의를 받지 않은 경우

● 회원 정보 입력	
회원 유형	<input checked="" type="radio"/> 개인 <input type="radio"/> 개인사업자 <input type="radio"/> 법인 <input type="radio"/> 비영리단체
* 이름	<input type="text"/> 성 <input type="text"/> 이름
* 주민등록번호	<input type="text"/> - <input type="text"/> <input type="button" value="실명확인"/>
본인 인증	상품 구매를 위해서는 본인인증이 필요합니다. 본인인증은 추후 my page > 회원 정보 관리에서 하실 수 있습니다. <input type="button" value="본인인증"/>

● 약관 동의	
웹 회원 약관	<input type="checkbox"/> 동의합니다.
제 1 장 총칙	
개인정보취급방침	<input type="checkbox"/> 동의합니다.
제 1 장 총칙	

점검 방법

- (1) 회원가입 등의 페이지가 있는지, 회원가입 등의 페이지가 없다고 하더라도 상담 게시판이나 이벤트 등을 이용하기 위해 개인정보를 입력하도록 하고 있는지 확인한다.
- (2) 개인정보를 수집하는 경우 개인정보 수집·이용에 대한 동의가 있는지 확인한다.
 - 개인정보 수집·이용 동의는 필수로 받도록 구현되어야 하고, 다른 항목들과 일괄 동의를 받지 않도록 구현되어야 한다.
 - 개인정보 수집·이용에 대한 동의 항목(개인정보의 수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간)을 고시해야 한다.
- (3) 개인정보를 제3자 제공 또는 처리위탁을 하는지 확인하고 이에 대한 동의가 제대로 되어 있는지 확인한다.
 - 제3자 제공 및 처리 위탁은 수집·이용 동의와 별도로 분리하여 동의를 받아야 하고,

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

제3자 제공 및 처리 위탁에 대해 동의하지 않더라도 서비스 가입이나 이용에 제한이 없도록 해야 한다.

- 단, 서비스 제공에 관한 계약을 이행하기 위해 필요한 업무의 경우에는 개인정보처리방침에 게시하면 동의 받지 않아도 된다.
- 제3자 제공 시 동의 항목 : 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
- 처리 위탁 시 동의 항목 : 개인정보 처리위탁을 받는 자, 개인정보 처리위탁을 하는 업무의 내용

(4) 고유식별정보나 민감정보를 수집하는지 확인하고, 수집할 경우 별도 동의를 받고 있는지 확인한다.

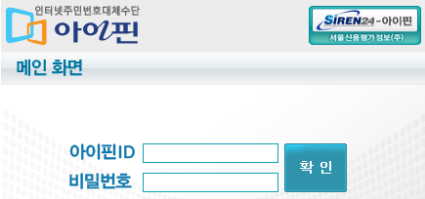
- 고유식별정보 및 민감정보를 수집하는 경우 기존 동의와 별도로 동의를 받아야 한다.

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

4. 주민등록번호 수집·이용 제한

준수 기준	<p>정보통신서비스 제공자는 다음에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없으며, 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.</p> <ol style="list-style-type: none"> 1. 본인확인기관으로 지정 받은 경우 2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우 3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우
관련 근거	<ul style="list-style-type: none"> • 정보통신망법 제 23 조의 2(주민등록번호의 사용 제한) • 개인정보보호법 제 24 조의 2(주민등록번호 처리의 제한)
미준수 시 벌칙	<ul style="list-style-type: none"> • 정보통신망법 - 주민등록번호를 수집·이용하거나 대체수단을 제공하지 않은 경우 : 3 천만원 이하의 과태료 • 개인정보보호법 - 주민등록번호를 처리, 대체 수단을 마련하지 않은 경우 : 5 천만원 이하의 과태료
<p>정보통신서비스 제공자는 정보통신망법에서 지정한 세가지 경우를 제외하고는 원칙적으로 인터넷 상에서 주민등록번호를 수집·이용 할 수 없으며, 주민등록번호를 사용하지 아니하고 본인을 확인할 수 있는 대체수단(아이핀, 휴대폰인증, 공인인증서 등)을 제공하여야 한다.</p> <p>주민등록번호를 사용한 회원가입 방법을 제공하고 있는 정보통신서비스 제공자는 정보통신망법 시행일(2012.8.18)부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 한다.</p>	
보호 조치	
<p>(1) 주민등록번호 수집·이용 금지</p> <p>주민등록번호를 반드시 사용해야 하는지 검토하여 불필요한 경우에는 주민등록번호를 삭제하고 처리하지 않도록 해야 한다.</p> <p>- 예) 웹사이트 회원가입 시 주민등록번호 미수집, 실명인증 및 본인확인 서비스 이용 시 주민등록번호 입력 금지</p>	
<p>(2) 대체수단 제공</p> <p>주민등록번호 수집·이용이 금지됨에 따라 실명인증 페이지 등을 포함하여 대체수단(아이핀, 공인인증서, 휴대폰 인증 등)을 제공해야 한다.</p>	

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7



아이핀ID

비밀번호

가입을 위한 본인 인증 방법을 선택해 주세요

이메일
휴대폰·유선전화

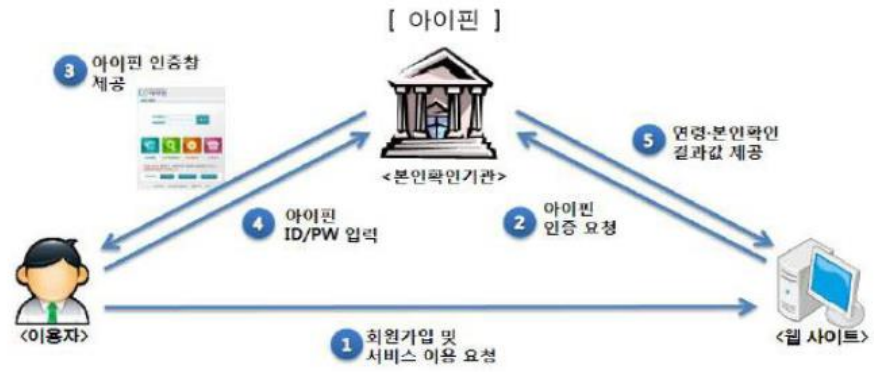
휴대폰·유선전화 입력 인증번호 받기

· 입력하신 휴대폰 또는 유선전화로 인증번호가 발송됩니다.
· 인증번호를 입력한 후 확인을 누르면 본인 인증이 완료됩니다.


[주요 주민등록번호 대체 수단]

대체수단	고객 입력값	시스템 저장값	대체 식별값 (연계정보포함)	비용(안)	서비스 가능일정
아이핀	ID,PW	이름,생년월일,DI,CI 등	DI,CI	유료	기 서비스중 (NICE,서신평,KCB)
휴대폰 본인확인	이름,생년월일, 폰번호,이통사정보	이름,생년월일, 폰번호,이통사정보,CI	CI 등 (기준미확정)	KT 고객 무료 타사 유료	이통 3 사 서비스 준비중 (방통위기준미확정)
공인인증서	이름,생년월일, 인증서 암호	이름,생년월일, SN,CI	CI 등 (기준미확정)	유료	2012.12 월 예상 (5 개사)


【 아이핀 】



【 휴대폰 인증 】



【 공인인증서 인증 】



미준수 예시

(1) [예시1] 회원가입 시 주민등록번호 수집

회원가입 시 주민등록번호가 필요하지 않지만 개인을 식별하기 위해 주민등록번호를

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

수집하는 경우

(2) [예시2] 본인확인 또는 실명 인증을 위하여 주민등록번호 사용

주민등록번호를 수집하여 저장하지 않으나, 실명 인증을 위하여 주민등록번호를 입력하는 경우

점검 방법

- (1) 주민등록번호를 수집 또는 이용하는 부분이 있는지 확인한다.
 - 예) 회원가입 시 주민등록번호 입력, 실명 인증을 위한 주민등록번호 입력 등
- (2) 주민등록번호 대체수단을 이용한 회원가입 또는 본인확인 등의 기능을 제공하고 있는지 확인한다.
 - 대체수단 : 아이핀, 공인인증서, 휴대폰인증 등

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

5. 개인정보 접속기록 저장 및 보관

준수 기준	<p>정보통신서비스 제공자 등은 접속기록의 위조·변조 방지를 위하여 다음의 조치를 하여야 한다.</p> <p>1. 개인정보처리자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속 일시, 처리내역 등의 저장 및 이의 확인·감독</p> <p>2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관</p>
관련 근거	<ul style="list-style-type: none">정보통신망법 제 28 조 (개인정보의 보호조치) 및 시행령 제 15 조 (개인정보의 보호조치)개인정보보호법 제 29 조(안전조치의 의무) 및 시행령 제 30 조(개인정보의 안전성 확보 조치)개인정보의 안전성 확보조치 기준(접속기록의 보관 및 점검)
미준수 시 벌칙	<ul style="list-style-type: none">정보통신망법 - 개인정보 접속기록 보호 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우 : 2 년 이하의 징역 또는 2 천만원 이하의 벌금(회사 : 위반행위와 관련한 매출액의 100 분의 3 이하에 해당하는 과징금)개인정보보호법 - 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 경우 : 2 년 이하의 징역 또는 2 천만원 이하의 벌금

개인정보처리자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속기록을 최소 1년 이상(다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상) 저장하고 월 1회 이상 정기적으로 확인·감독 하여야 한다.

접속기록 항목으로는 정보주체 식별정보, 개인정보처리자 식별정보, 접속 일시, 접속지 정보, 부여된 권한 유형에 따른 수행업무 등을 포함해야 한다.

개인정보처리시스템의 접속기록이 위·변조되지 않도록 별도 저장 장치에 백업 보관해야 한다.

[접속기록 항목 예시]

정보주체식별정보	처리자식별정보	접속 일시	접속지	수행업무
123456789	홍길동(HGD)	2012.06.03 15:00:00	172.168.168.11	조회(고객응대)

보호 조치

(1) 개인정보 처리내역에 대한 접속기록 저장

개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속기록(정보주체 식별정보, 개인정보처리자 식별정보, 접속 일시, 접속지 정보, 부여된 권한 유형에 따른 수행업무 등)을

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

1년 이상(다만, 5만명 이상의 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상)

(2) 접속기록에 대한 정기적 확인·감독

접속기록을 월 1회 이상 정기적으로 확인·감독해야 한다.

(3) 개인정보 접속기록 위·변조 방지 조치

개인정보처리자의 접속기록이 위·변조되지 않도록 별도의 물리적 저장 장치(예. CD-ROM, WORM 스토리지 등)에 보관해야 한다.

미준수 예시

(1) [예시1] 개인정보 접속기록 로그를 남기지 않고 있음

개인정보 등록/조회/수정/삭제 등의 메뉴에 대해 접속기록을 로그로 남기지 않는 경우

(2) [예시2] 개인정보 접속기록 로그를 3개월만 보관

저장공간 부족으로 개인정보 접속기록에 대한 로그를 3개월만 보관하고 있는 경우

(3) [예시3] 개인정보 접속기록을 별도 보관하지 않고 있음

개인정보 접속기록을 별도의 저장장치에 보관하지 않아 접속기록이 위·변조 될 가능성이 있는 경우

점검 방법

(1) 개인정보를 등록/조회/수정/삭제 등의 메뉴가 있는지 확인한다.

(2) 개인정보 처리 메뉴가 존재하는 경우, 접속기록 로그를 남기고 있는지 확인한다.

- 접속기록 항목 : 정보주체 식별정보, 개인정보처리자 식별정보, 접속 일시, 접속지 정보, 부여된 권한 유형에 따른 수행업무 등을 포함해야 함

(3) 개인정보 접속기록을 1년 이상 보관하고 위·변조되지 않도록 처리하고 있는지 확인한다.
(다만, 5만명 이상의 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상)

(4) 접속기록을 월 1회 이상 정기적으로 확인·감독하고 있는지 확인한다.

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

6. 개인정보 숨김처리

준수 기준	시스템 및 프로그램의 목적 및 용도에 따라 숨김처리(개인정보 표시제한)를 적용하여 개인정보 유·노출을 최소화 하여야 한다.
관련 근거	<ul style="list-style-type: none"> 정보통신망법 제 28 조 (개인정보의 보호조치) 및 시행령 제 15 조 (개인정보의 보호조치) 개인정보보호법 제 29 조(안전조치의 의무) 및 시행령 제 30 조(개인정보의 안전성 확보 조치)

개인정보 업무 처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보 보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취하는 경우 다음의 숨김처리 기준을 준용하여야 한다.

보호 조치

(1) 개인정보 조회, 출력 시 개인정보 항목별 다음의 숨김처리 기준에 따라 처리하여야 한다.

항목	숨김처리 기준
고객명	뒤1글자(글자수 상관없이 뒤1글자 마스킹)
예금주	뒤1글자(글자수 상관없이 뒤1글자 마스킹)
카드소유자	뒤1글자(글자수 상관없이 뒤1글자 마스킹)
번호예약자	뒤1글자(글자수 상관없이 뒤1글자 마스킹)
주민번호	뒤6글자
해지주민번호	뒤6글자
외국인등록번호	뒤6글자
여권번호	뒤4글자
생년월일	미적용
이동전화	국번 뒤2글자, 번호 앞1글자 (000-00**-*(000))
연락전화	상동
우편번호	미적용
주소	(구)번지부터, (신)도로명 이후부터
직업	미적용
e-mail	뒤3글자
계좌번호	앞6글자 표기
신용카드(결제 기능 있는 카드 포함) (예. 신용카드 기능이 있는 월드패스(선불), 멤버십번호)	앞6글자, 뒤1글자 표기
카드유효일	모두
신용조회결과	미적용

문서명	개인정보보호 가이드
작성일자/버전	2019-08/Ver1.7

단말기번호	모두(권한자에게만 표기)
IMEI	모두(권한자에게만 표기)
ESN	모두(권한자에게만 표기)
IMSI	모두(권한자에게만 표기)
USIM번호	모두(권한자에게만 표기)
멤버십번호 (예. 올레클럽)	개인 식별 불가 수준 마스킹(자체 내부지침 생성, 적용)
인터넷ID	뒤3글자
시스템ID(시스템 내부적으로 생성한 개인(고객)을 식별할 수 있는 고유값) (예. sa_id, cust_id, ia_id 등)	뒤3글자
패스워드	모두
IP	첫째/셋째 3자리씩
외국인 이름(성+이름)	전체 자리수 기준, 뒤 1/3 글자수
운전면허번호	가운데6글자

미준수 예시

(1) [예시1] 비밀번호 일부 또는 전체가 평문으로 보여줌

비밀번호 항목은 모두 숨김처리 표시하여야 하나, 일부 또는 전체를 그대로 보여주는 경우

(2) [예시2] 주민등록번호 전체를 평문으로 보여줌

주민등록번호는 성별 뒤 6자리를 숨김처리 표시하여야 하나, 일부 또는 전체를 모두 보여주는 경우

점검 방법

- (1) 주민번호, 비밀번호 등 주요 개인정보를 처리하고 있는지 확인한다.
- (2) 주요 개인정보를 처리하고 있는 경우 개인정보를 조회, 출력 하는 메뉴가 있는지 확인한다.
- (3) 개인정보를 조회, 출력하는 메뉴에서 각 항목별 숨김처리 기준을 준수하고 있는지 확인한다.