2020년 상반기 개인정보처리업무 수탁업체 교육

2019. 10

당신에게 좋은보험 삼성화재

CONTENTS

1. 업무 위수탁 관련 법규
2. 개인정보 유출 사고 대응 방안
3. 개인정보 보호 상담 사례를 통한

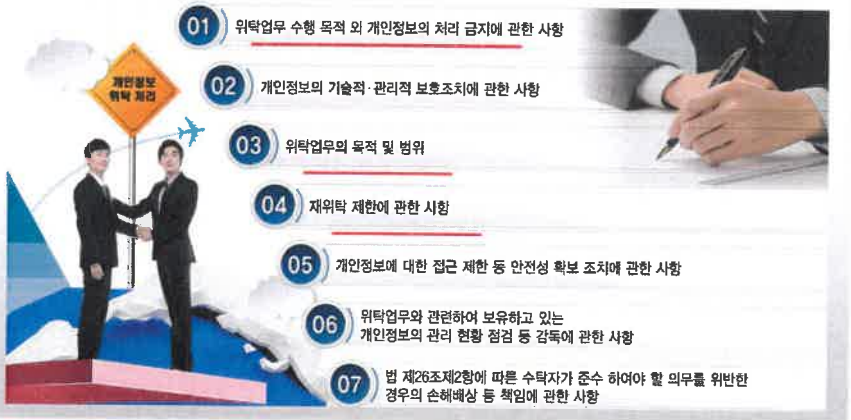
당신에게 좋은보험 삼성화재

1. 업무 위수탁 관련 법규

당신에게 좋은보험 삼성화재

개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)제1항

개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다



01 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

02 개인정보의 기술적·관리적 보호조치에 관한 사항

03 위탁업무의 목적 및 범위

04 재위탁 제한에 관한 사항

05 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항

06 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항

07 법 제26조제2항에 따른 수탁자가 준수 하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

당신에게 좋은보험 삼성화재

3

개인정보보호법 제26조에 따른 재위탁 제한에 관한 법률

개인정보보호법 제 19조(개인정보를 제공받은 자의 이용·제공 제한)

개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1.정보주체로부터 별도의 동의를 받은 경우

2.다른 법률에 특별한 규정이 있는 경우

개인정보보호법 제 26조 제5항(업무 위탁에 따른 개인정보의 처리 제한)

수탁자는 개인정보처리자로부터 위탁 받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니된다.

개인정보보호법 시행령 제28조 제1항 제2호(개인정보 처리 업무 위탁 시 조치)

법 제26조제1항 제3호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.

2. 재위탁 제한에 관한 사항

정보통신망법 제25조 제7항(개인정보 처리 위탁)

수탁자는 개인정보 처리 위탁을 한 정보통신서비스 제공자 등의 동의를 받은 경우에 한하여 제1항에 따라 위탁 받은 업무를 제3자에게 재위탁할 수 있다.

개인정보처리 재위탁 동의

정보통신망법 개정으로 협력사가 재위탁을 하기 전에 당사의 동의를 얻어야 함

정보통신망법 제25조(개인정보의 처리 위탁)

⑦ 수탁자는 개인정보 처리 위탁을 한 정보통신서비스 제공자 등의 동의를 받은 경우에 한하여 제1항에 따라 위탁 받은 업무를 제3자에게 재위탁할 수 있다.

재위탁 개요

재위탁 사전동의 위반, 재위탁 관리감독 소홀로 인한 사고 발생 시

협력사에서 재위탁 사전 동의 위반, 재위탁 관리감독 소홀로 인한 사고 발생 시 협력사는 과태료, 위탁사는 과징금 처분(정보통신망법 제76조 제2항 1의2호, 제64조의 3 제1항 5의2호)

※ 사고발생 시 민, 형사상 책임은 별도 존재 함.

당신의 힘 개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)제4항

- 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리 하는지를 감독하여야 한다

수탁자 선정
수탁자를 선정할 때에는 인력과 물적 시설, 재정 부담능력 등을 종합적으로 고려하여야 한다

수탁자 처리 업무 지연
개인정보처리자는 수탁자의 처리 업무의 지연, 처리 업무와 관련없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련해야 하여야 한다

위탁 개인정보 보호
수탁자는 위탁받은 개인정보를 보호하기위하여 「개인정보의 안전성 확보조치 기준」에 따라 관리적·기술적·물리적 조치를 하여야 한다

당신의 힘 개인정보보호법 제29조(안전조치의무)

- 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다

01 내부관리계획의 수립·시행
02 접근권한의 관리
03 접근통제
04 개인정보의 암호화
05 접속기록의 보관 및 점검
06 악성프로그램 등 방지
07 물리적 접근 방지
08 개인정보의 파기

※ 출처 : 개인정보의 안전성 확보 조치 기준 [시행 2019.06.07.] [행정자치부고시 제2019-47호, 2019.06.07.]

개인정보 유출사고 손해배상

❖ 정통망법 징벌적 손해배상제도(제32조) 와 법정 손해배상제도(제32조의 2)

구분	징벌적 손해배상제도	법정 손해배상제도
적용 요건	기업의 고의·중과실로 개인정보 유출 또는 동의없이 활용하여 피해 발생	기업의 고의·과실로 개인정보가 분실·도난·유출된 경우
입증 책임	기업이 고의·중과실 없음을 입증 피해액은 피해자가 입증	기업이 고의·과실 없음을 입증 피해자에 대한 피해액 입증책임 면제
구제 범위	재산 및 정신적 피해 모두 포함	사실상 피해 입증이 어려운 정신적 피해
배상 규모	실제 피해액의 3배 이내 배상	300만원 이하의 범위에서 상당한 금액
적용 시기	2016년 7월 25일 이후 유출사고	

개인정보 유출이란?

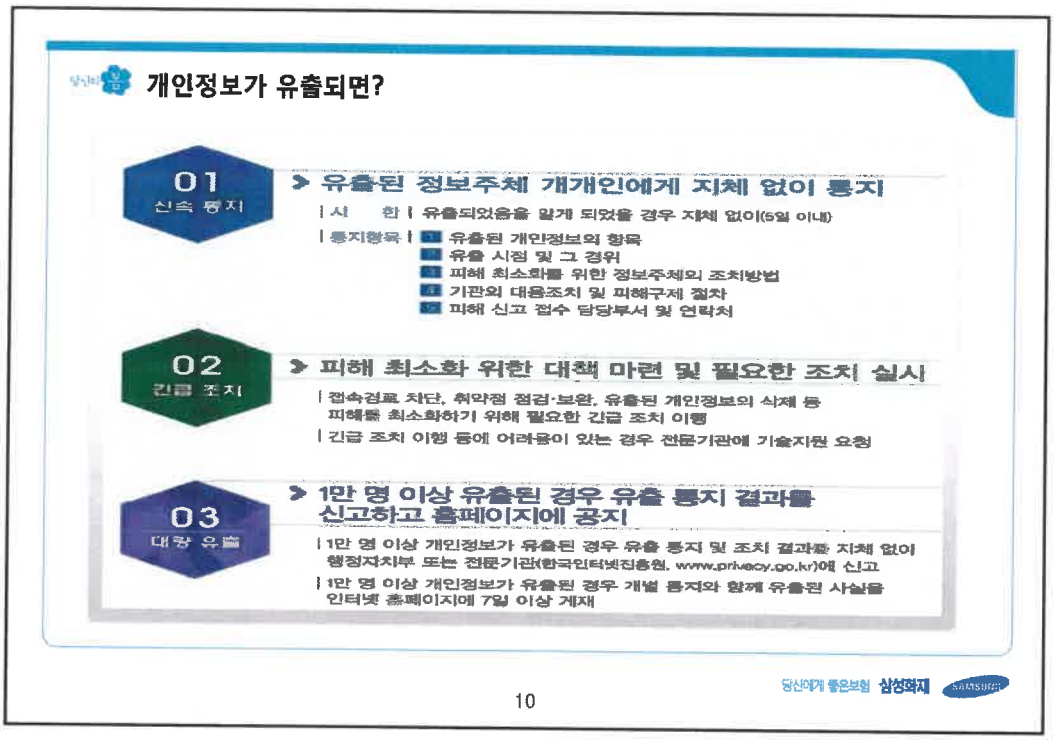
- 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보 처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 경우

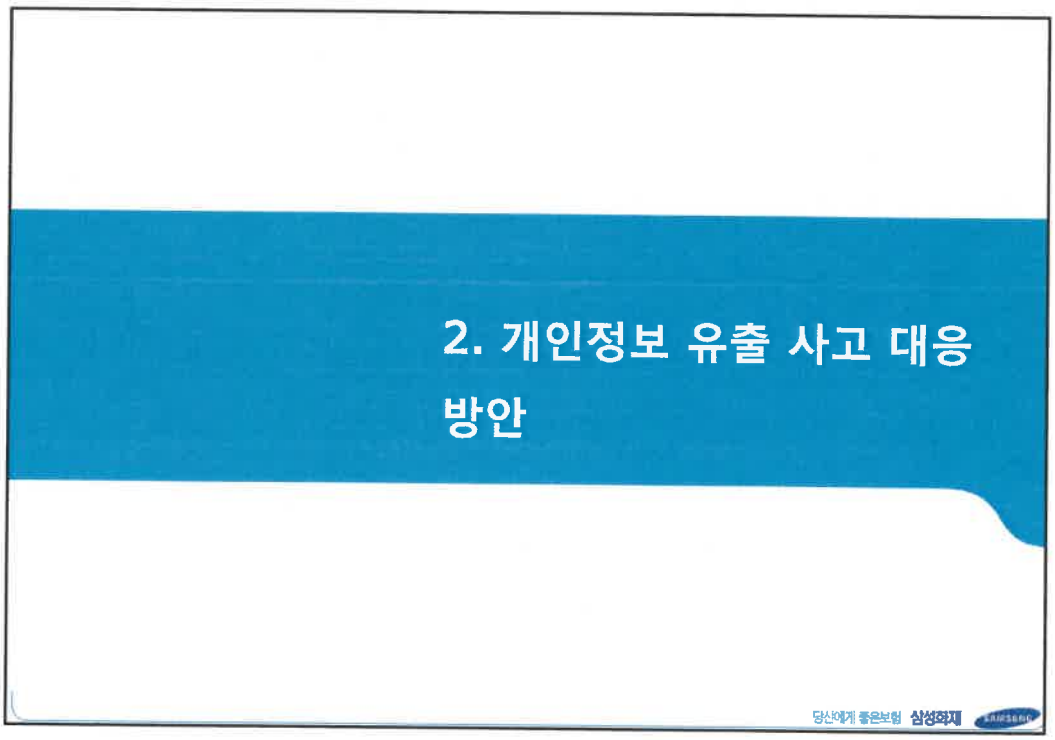
01 개인정보가 포함된 서면, 이동식 저장장치, 휴대용컴퓨터 등을 분실 또는 도난당한 경우

02 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

03 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우

04 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우


개인정보가 유출되면?
01
신속 통지
유출된 정보주체 개개인에게 지체 없이 통지
시 한 | 유출되었음을 알게 되었을 경우 지체 없이(5일 이내)
통지항목 | 1. 유출된 개인정보의 항목
2. 유출 시점 및 그 경위
3. 피해 최소화를 위한 정보주체의 조치방법
4. 기관의 대응조치 및 피해구제 절차
5. 피해 신고 접수 담당부서 및 연락처
02
긴급 조치
피해 최소화 위한 대책 마련 및 필요한 조치 실시
| 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급 조치 이행
| 긴급 조치 이행 등에 어려움이 있는 경우 전문기관에 기술지원 요청
03
대량 유출
1만 명 이상 유출된 경우 유출 통지 결과를 신고하고 홈페이지에 공지
| 1만 명 이상 개인정보가 유출된 경우 유출 통지 및 조치 결과를 지체 없이 행정자치부 또는 전문기관(한국인터넷진흥원, www.privacy.go.kr)에 신고
| 1만 명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재
당신에게 좋은보험 삼성화재
10


2. 개인정보 유출 사고 대응 방안
당신에게 좋은보험 삼성화재

개인정보 유출 · 침해사고 예방을 위한 조치

예방 수칙

⊖ 개인정보 최소 수집 및 파기
⊖ 법률에서 요구하는 의무사항 이행
⊛ 관리자페이지는 반드시 보안설정
④ 주기적 점검(내부, 외부)은 필수

개인정보보호법 제29조(안전조치 의무)

개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.

정보통신망법 제28조(개인정보의 보호조치)

정보통신서비스 제공자 등이 개인정보를 처리할 때에는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적 · 관리적 조치를 하여야 한다.

개인정보 안전성 확보 조치 기준(개정)

내부 관리 계획의 수립·시행

○ 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 내부 의사 결정 절차를 통하여 다음의 사항을 포함하는 내부 관리계획을 수립 · 시행

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근 권한의 관리에 관한 사항
5. 접근 통제에 관한 사항
6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보 보호를 위하여 필요한 사항

○ 위의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리

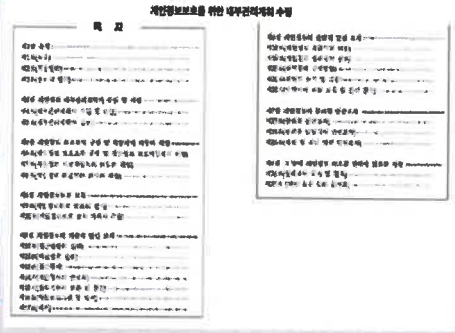
○ 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리 계획의 이행 실태를 연1회 이상 점검·관리

개인정보 안전성 확보 조치 기준(개정)

[사례] 내부 관리계획 미수립 위반

위반사항

- ✓ A병원은 30만건 이상의 개인정보를 수집·보관하고 있었으나,
- ✓ 유형에 따른 필수사항을 포함하지 않고 의무 업무와 관련된 내용만 내부관리계획으로 관리하고 있었음



조치사항

- ✓ 개인정보처리자 내부 의사 결정 절차를 통하여 내부 관리계획 수립·시행

조치 TIP ▪ 개인정보보호 종합 포털에서 제공하는 개인정보 내부 관리계획 샘플 참고

개인정보 안전성 확보 조치 기준(개정)

접근 권한의 관리

- 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한 범위로 업무 담당자에 따라 차등 부여 (유형1은 아니할 수 있음)
- 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한 변경 또는 말소
  - 권한 부여, 변경 또는 말소에 대한 내역 기록하고, 그 기록 최소 3년간 보관
- 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 사용자계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 조치
- 개인정보취급자 또는 정보주체가 안전한 비밀번호 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용
- 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근 제한하는 등 필요한 기술적 조치 (유형1은 아니할 수 있음)

개인정보 안전성 확보 조치 기준(개정)

[사례]접근권한 부여, 변경, 말소 이력 보관 미흡

위반사항

- ✓ A사는 생활용품을 개발·제조·판매하는 온라인 쇼핑몰을 운영하고 있음
- ✓ 쇼핑몰 회원 가입시 고객들의 개인정보를 수집하였고 이를 관리하는 개인정보보호 담당자를 지정·관리하고 있었음
- ✓ 개인정보보호 담당자에게 권한을 부여·수정·삭제한 이력에 대해서 최근 1년의 내역만 보관하고 있었음

조치사항

- 개인정보처리자는 개인정보보호 담당자 권한 부여·변경·말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관

당신에게 좋은보험 삼성화재

16

개인정보 안전성 확보 조치 기준(개정)

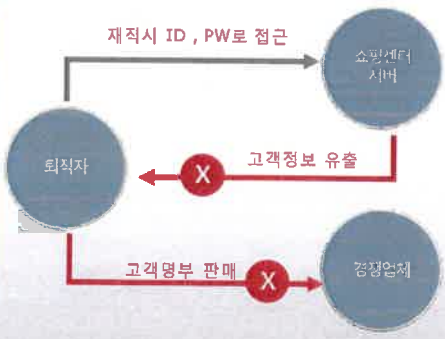
[사례] 퇴직자의 접근권한 방지

위반사항

- ✓ 퇴직한 직원의 계정이 방치되어 있는 상태에서 해당 계정으로 개인정보처리 시스템에 접근하여 개인정보 유출

조치사항

- ✓ 퇴직한 직원의 계정 접근권한 회수, 사용중지 처리



당신에게 좋은보험 삼성화재

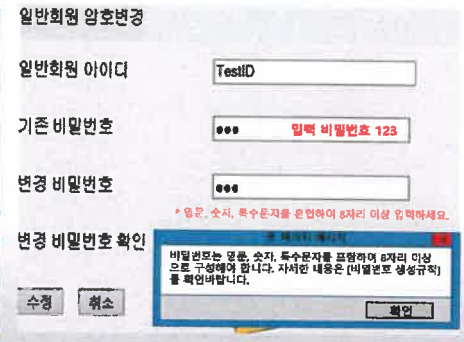
17

개인정보 안전성 확보 조치 기준(개정)

[사례] 비밀번호 작성 규칙 미수립 위반

위반사항

- ✓ B업체는 호텔·콘도·스키장·골프장 등 종합 레저 사업을 하는 업체로, 개인정보처리 시스템을 도입해 개인정보를 저장·운용하고 있다.
- ✓ 그러나 B업체는 개인정보처리 시스템 로그인할 때 비밀번호 작성 규칙 수립 및 적용이 되어 있지 않았다.



조치사항

- 비밀번호 작성 규칙 수립 및 적용
  (비밀번호는 문자, 숫자 등으로 조합·구성)

조치 TIP

- 암호이용활성화 홈페이지(https://seed.kisa.or.kr)에서 제공하는 "패스워드 선택 및 안내서" 및 비밀번호 안전성 검증 소프트웨어 활용

개인정보 안전성 확보 조치 기준(개정)

접근 통제

○ 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음의 기능을 포함한 조치

- ✓ **개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한**
- ✓ **개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응**

*** 침입차단 및 침입탐지 정책 설정, 개인정보처리시스템에 접속한 이상 행위 대응, 로그 훼손 방지 등 적절한 운영·관리가 필요**

○ 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우
안전한 접속 수단을 적용하거나 안전한 인증 수단을 적용

* 안전한 접속수단 : 가상사설망(VPN), 전용선 등
* 안전한 인증수단 : 인증서(PKI), 보안토큰, 일회용비밀번호(OTP) 등

개인정보 안전성 확보 조치 기준(개정)

접근 통제

- 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등 통하여 열람권한이없는 자 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치
- 인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우 연 1회 이상 취약점을 점검하고 필요한 보완 조치

- 개인정보처리시스템에 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속 차단 조치
- 업무용 모바일 기기의 분실,도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 조치

개인정보 안전성 확보 조치 기준(개정)

개인정보의 암호화

구 분				암호화 기준
정보통신망, 보조저장매체등 통한 송신 시	비밀번호, 바이오정보, 고유식별정보			암호화 송신
개인정보처리시스템에 저장 시	비밀번호			일방향(해쉬 함수) 암호화 저장
	바이오정보			암호화 저장
	고유식별정보	주민등록번호		암호화 저장
		여권번호, 외국인 등록번호, 운전면허번호	인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)	암호화 저장
			내부망에 저장	※ 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ※ 암호화 미적용시 취약도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장시	비밀번호, 바이오정보, 고유식별정보			※ 비밀번호는 일방향 암호화 저장 ※ 상용 암호화 소프트웨어 또는 안전한 알고리즘 암호화

- 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장
- 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장
  안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행

개인정보 안전성 확보 조치 기준(개정)

[사례] 관리자 계정 비밀번호 저장 미흡

위반사항

- ✓ A병원은 관리자 계정, 환자들 계정에 대한 비밀번호를 암호 알고리즘으로 암호화하지 않은 채 평문으로 저장하고 있었음

조치사항

- 비밀번호 저장 시 복호화 되지 않도록 일방향 암호화 적용

조치 TIP

- KISA 암호기술 및 정책 자료(https://seed.kisa.or.kr/kisa/reference/EgovGuide.do) 참고

개인정보 안전성 확보 조치 기준(개정)

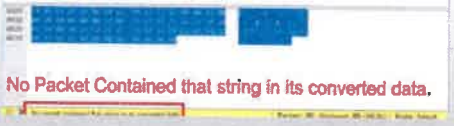
[사례] 개인정보처리시스템 비밀번호 전송 구간 암호화 미적용

위반사항

- ✓ A학교는 소속 학생, 비소속 학생과 일반인 대상으로 교육 서비스 제공
- ✓ 해당 서비스 제공 과정은 홈페이지를 통해서만 접수 가능, 수강 종료 후 학위 자격증 확인을 위해 수강생 개인정보를 준영구적으로 보관하고 있음

조치사항

- 고유식별정보, 비밀번호, 바이오 정보를 정보통신망을 통하여 송신하는 경우 암호화 적용



개인정보 안전성 확보 조치 기준(개정)

접속기록의 보관 및 점검

○ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 안전하게 보관 · 관리 5만명 이상, 고유식별정보 또는 민감 정보 처리 시 2년 이상 보관 · 관리

○ 개인정보처리시스템의 접속기록 등을 월1회 이상 점검, 특히 개인정보 다운로드 발견 시 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 함

개인정보 안전성 확보 조치 기준(개정)

접속기록의 보관 및 점검

○ 개인정보처리시스템에 대한 개인정보 입·출력 및 수정, 파일별·담당자별 데이터 접근 내역 등을 자동으로 기록하는 로그 파일을 생성하여 최소 1년 이상 보관 및 관리

접속기록 일정기간 저장·관리할 수 있도록 개발

❖ 필수 기록 항목

- 계정 : (개인정보취급자 식별정보) ID 등
- 접속 일시 : 날짜 및 시간
- 접속지 정보 : 접속자 정보(IP 주소 등)
- 처리한 정보주체 정보 : 고객번호, 사번 등
- 수행 업무 : 열람, 수정, 삭제, 인쇄 입력 등

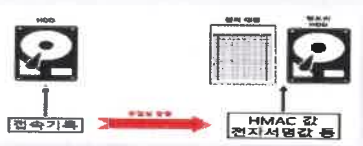
접속기록 항목 (예시)

취급자 식별정보	정보주체 식별정보	접속일시	접속지	수행업무
홍길동	성춘향	20XX.04.18 15:00:00	172.168.11.11	노출교육 신청

접속기록 백업

❖ 별도 물리적인 저장 장치에 보관하고 정기적인 백업 수행

- 접속기록 위 · 변조 방지를 위해 CD-ROM 같은 덮어쓰기 방지 매체 사용
- 수정 가능한 매체 백업 시, 위 · 변조 여부를 확인할 수 있는 정보(HMAC or 전자서명 등)를 별도 장비에 보관 · 관리



개인정보 안전성 확보 조치 기준(개정)

[사례] 처리시스템 접속기록 항목 누락

위반 사항

- ✓ A기관은 주택 건설, 토지 개발 등의 공공업무를 수행하는 기관으로 분야별 사업 특성에 따라 수집·저장하는 개인정보도 달랐고, 그것을 보관 관리하는 개인정보처리시스템 또한 여러 개로 분리 될 수밖에 없었음
- ✓ 총5개의 개인정보처리시스템은 운용하고 있었는데, 그 중 2개의 시스템의 경우 개인정보취급자 ID 및 수행 업무에 대해 기록하고 있지 않았음

조치사항

- 개인정보처리시스템에 접속한 기록을 보관할 때 필수 항목을 기록·보관

당신에게 좋은보험 삼성화재

개인정보 안전성 확보 조치 기준(개정)

악성프로그램 등 방지

○ 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영

악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시

보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지

발견된 악성프로그램 등에 대해 삭제 등 대응 조치

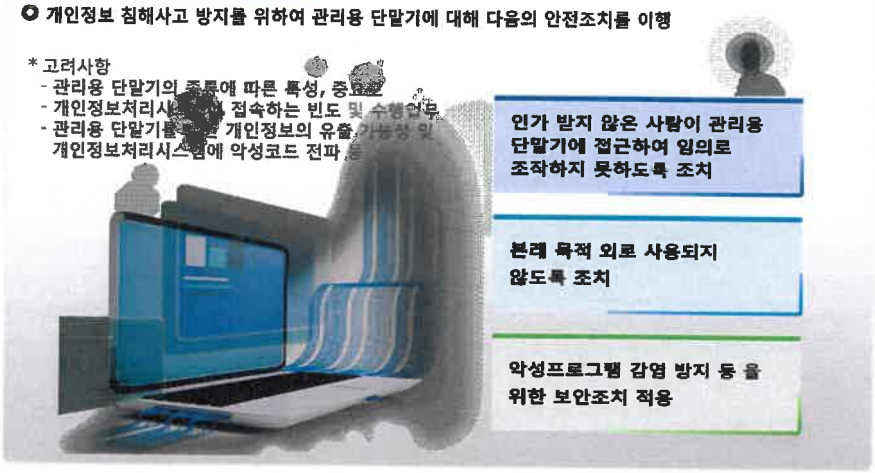
당신에게 좋은보험 삼성화재

개인정보 안전성 확보 조치 기준(개정)

관리용 단말기의 안전조치

○ 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음의 안전조치를 이행

* 고려사항
- 관리용 단말기의 종류에 따른 특성, 중요도
- 개인정보처리시스템에 접속하는 빈도 및 수행업무
- 관리용 단말기를 통한 개인정보의 유출 가능성 및 개인정보처리시스템에 악성코드 전파 등



인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치

본래 목적 외로 사용되지 않도록 조치

악성프로그램 감염 방지 등 을 위한 보안조치 적용

개인정보 안전성 확보 조치 기준(개정)

모바일기기에 대한 안전조치

1. 의심스러운 애플리케이션 다운로드 금지
2. 신뢰할 수 없는 사이트 방문 금지
3. 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제
4. 비밀번호 설정 기능 및 관리
5. 블루투스 기능 등 무선 인터페이스 관리
6. 이상 증상이 지속될 경우 악성코드 감염 여부 확인
7. 다운로드한 파일은 바이러스 유무 검사 후 사용
8. 정기적인 바이러스 검사
9. 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트

개인정보 안전성 확보 조치 기준(개정)

물리적 안전조치

- 전산실, 자료보관실 등 개인정보 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우 이에 대한 **출입통제 절차를 수립·운영**

- 개인정보가 포함된 **서류, 보조저장매체 등을 잠금장치**가 있는 안전한 장소에 보관

- 개인정보가 포함된 **보조저장매체의 반출·입 통제를 위한 보안대책을 마련**
  - 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있음

개인정보 안전성 확보 조치 기준(개정)

개인정보의 파기

- 개인정보를 파기할 경우 다음 어느 하나의 조치를 하여야 함

전체 파기

완전파괴 (소각·파쇄 등)

전용 소자장비 이용하여 삭제

데이터가 복원되지 않게 초기화 또는 덮어쓰기

- 개인정보의 일부만을 파기하는 경우 위의 방법으로 파기하는 것이 어려울 때에는 다음의 조치를 하여야 함

일부파기

전자적 파일 형태인 경우	제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우
개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독	해당 부분을 마스킹, 천공 등으로 삭제

개인정보 안전성 확보 조치 기준(개정)

개인정보의 파기

○ 개인정보를 파기할 경우 다음 어느 하나의 조치를 하여야 함

전체 파기

완전파괴
(소각·파쇄 등)

전용 소자장비
이용하여 삭제

데이터가 복원
되지 않게 초기화
또는 덮어쓰기

○ 개인정보의 일부만을 파기하는 경우 위의 방법으로 파기하는 것이 어려울 때에는 다음의 조치를 하여야 함

일부 파기

전자적 파일 형태인 경우

개인정보를 삭제한 후 복구 및
재생되지 않도록 관리 및 감독

**제1호 외의 기록물, 인쇄물,
서면, 그 밖의 기록매체인 경우**

해당 부분을 마스킹, 천공 등으로 삭제

당신에게 좋은보험 삼성화재

32

삼성화재 수탁 업체 관리 방안

보안부서 주관

- 개인정보 관리 및 IT보안 전반에 걸친 보안 수준 점검
  1. 연 1회 점검
  2. 정보보안 관리체계(10개 항목), 네트워크(8개 항목),
     고객정보처리시스템(19개 항목), PC보안(24개 항목)
  3. 점검 결과에 따른 보안 컨설팅 제공

현업부서 주관

- 개인정보파기확인서 징구(월 1회)
- 교육 점검 실시(반기 1회)
  - 19년 하반기부터 축소 운영, 기본 분기 1회 실시

당신에게 좋은보험 삼성화재

33

3. 개인정보 보호 상담 사례를 통한 Q&A

당신에게 좋은보험 삼성화재

개인정보 상담 사례를 통한 Q&A

차량번호 하나만으로는 개인정보라고 볼 수 없나요?

A 구체적으로 해당 차량번호가 수집 및 이용되는 상황에 따라 판단이 달라질 수 있지만 차량 번호 하나만으로는 개인을 식별할 여지가 없더라도 자동차등록원부 등과 쉽게 결합하여 등록자 개인을 식별할 수 있으므로 개인정보로 볼 수 있습니다.

참고

주요 개념 정의

- 개인정보파일: 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)
- 개인정보 처리: 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위
- 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
- 개인정보처리자: 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등

당신에게 좋은보험 삼성화재

개인정보 상담 사례를 통한 Q&A

Q2 차량번호 하나만으로는 개인정보라고 볼 수 없나요?

A 구체적으로 해당 차량번호가 수집 및 이용되는 상황에 따라 판단이 달라질 수 있지만 차량번호 하나만으로는 개인을 식별할 여지가 없더라도 자동차등록원부 등과 쉽게 결합하여 등록자 개인을 식별할 수 있으므로 개인정보로 볼 수 있습니다.

참고

주요 개념 정의

- 개인정보파일: 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)
- 개인정보 처리: 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위
- 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
- 개인정보처리자: 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등

개인정보 상담 사례를 통한 Q&A

스마트폰에 저장된 전화번호 단독으로도 개인정보로 볼 수 있나요?

A 전화번호는 단독으로도 개인정보가 될 수 있습니다. 단, 「개인정보 보호법」 상 의무를 부담하는 대상(개인정보처리자)은 업무를 목적으로 개인정보를 처리하는 경우에 한정됩니다.
사적인 친분관계를 위하여 스마트폰에 전화번호, 이메일 등을 저장하는 경우는 개인정보처리자에 해당하지 않습니다.

참고

생존하는 특정 개인을 알아볼 수 있는 정보

- 특정 개인을 알아볼(식별할) 수 있는 정보로, 해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 식별 가능하다면 개인정보에 해당됨
- 가령, 성명 정보만 있다면 특정 개인을 식별하는 것이 쉽지 않으나(동명이인 등), 주소, 연락처 등과 결합되어 특정한 개인을 식별할 수 있다면 개인정보로 볼 수 있음

개인정보 상담 사례를 통한 Q&A

내부 직원에 대한 교육을 외부 업체에 위탁할 때 위탁에 대한 동의를 받아야 하나요?

A 「표준 개인정보보호 지침」에서는 근로자와 사용자가 근로계약을 체결하는 경우, 임금지급, 교육, 증명서 발급, 근로자 복지 등을 위하여 근로자 동의 없이 개인정보를 수집·이용할 수 있도록 규정하고 있습니다. 따라서 내부 직원에 대한 교육위탁은 별도 동의는 필요하지 않지만, 위탁내용과 수탁자는 고지해야 합니다.

참고

위탁 업무 등의 공개 방법

- 위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법
- 관보(위탁자가 공공기관인 경우로 한정한다)나 위탁자의 사업장등이 소재하는 시 · 도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호 · 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
- 동일한 제호로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물 · 소식지 · 홍보지 · 청구서 등에 지속적으로 싣는 방법
- 재화 또는 용역을 제공하기 위한 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 게 발급하는 방법

개인정보 상담 사례를 통한 Q&A

비밀번호는 반드시 8자리 이상으로 설정해야 하나요?

A 「개인정보의 안전성 확보조치 기준」 제5조에 따르면, 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하도록 하고 있습니다.
즉, 안전하지 못한 비밀번호를 사용할 경우 정보가 노출될 위험성이 있으므로, 생일, 전화번호 등 추측하기 쉬운 숫자나 문자 등을 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 개인정보처리시스템에 적용하여야 합니다.
이 때 비밀번호의 최소 길이는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 합니다. 참고로 비밀번호 작성규칙은 아래와 같습니다.

참고

비밀번호 작성규칙

- 최소 10자리 이상: 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 2종류 이상으로 구성
- 최소 8자리 이상: 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9개, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성

개인정보 상담 사례를 통한 Q&A

3-6 SNS 채팅방 개인정보 노출

Q 승무원 학원 업체 직원이 1000여명의 某 항공사 지원자 명단 파일을 SNS 오픈 채팅방에 게시하여 지원자 개인정보 다수가 노출되었습니다.

A 개인정보처리자는 노출된 개인정보 파일이 더 이상 유포되지 않도록 삭제 등의 필요한 조치를 취하여야 합니다.

개인정보처리자는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 합니다.

이 사례의 경우 업무담당자가 업무 수행을 하는 과정에서 개인정보가 포함된 파일을 정당한 권한이 없는 자가 접근할 수 있는 SNS 오픈채팅방에 업로드하면서 개인정보가 노출되었습니다. 우선 개인정보가 포함된 엑셀 파일을 삭제하여야 하고, 해당 페이지 접속자 수 및 파일 다운로드 건수 등을 파악하여 노출 현황을 파악하여야 합니다. 그리고 만약 해당 파일이 노출되었다면 구글 검색 엔진 등을 통해 해당 정보가 인터넷 상에 유포되었는지 유무를 확인하여 해당 검색엔진 업체 등에 개인정보 삭제를 요청하여야 합니다.

- 수탁업체에서 업무 편의를 위해 고객에게 개인정보가 담긴 사진(주민등록증, 운전면허증, 통장 사본, 차량등록증 등등) 개인 SNS 채팅방(카카오톡, 네이트온, 밴드)를 통해 개인정보 수집
- 이러한 정보를 업무 효율 상 쉽게 공유하기 위해 개인 SNS 단체 채팅방에 공유
- 업무용PC에 업로드, 출력을 위해 본인 SNS채팅창으로 사진 전송
- 개인정보 목적 달성 후 삭제 되어야 할 개인정보 SNS 채팅창에 존재함.

개인정보 상담 사례를 통한 Q&A

4-1 개인정보 파기 시점

Q 더 이상 이용하지 않은 사이트의 회원 탈퇴를 하려 합니다. 그런데 탈퇴 후 개인정보 파기와 관련해서 회원가입시 동의한 내용과 회사에서 말하는 파기 시점이 제 각각입니다. 회원탈퇴 후 언제 개인정보가 파기되어야 하는 건가요?

A 개인정보 수집·이용에 대해 동의시 고지된 보유기간이 경과하면 파기하여야 합니다.

개인정보처리자는 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기해야 한다. "개인정보가 불필요하게 되었을 때"란 개인정보의 처리목적이 달성되었거나, 해당 서비스의 폐지, 사업이 종료된 경우 등이 포함됩니다. 다만 다른 법령에 따라 보존하여야 하는 경우에는 파기하여서는 안 됩니다.

〈"개인정보가 불필요하게 되었을 때" 경우 예시〉

① 개인정보처리자가 당초 고지하고 동의를 받았던 보유기간의 경과
② 동의를 받거나 법령 등에서 인정된 수집·이용·제공 목적의 달성
③ 계명, 계약관계 종료, 동의철회 등에 따른 개인정보처리의 법적 근거 소멸
④ 개인정보처리자의 폐업·청산
⑤ 대금 완제일이나 채권소멸시효기간의 만료

이 사례의 경우 회원 가입시 개인정보 수집·이용에 대한 동의시 당초 고지 받았던 보유기간이 있다면 해당 보유기간이 경과하면 개인정보를 파기하여야 합니다. 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그때로부터 5일 이내에 해당 개인정보를 파기하여야 합니다.

- 위·수탁사 개인정보 파기 이해 시점이 상이함

  ex) 위탁사 : 보고서 업로드 일로부터 5일 이내 삭제

  수탁사 : 수임료 입금일로부터 5일 이내 삭제

- 개인정보의 처리 목적이 달성되어 삭제 해야 하는 개인정보를 현업 담당자가 추후 되묻는 경우를 대비해 삭제 하지 않는 경우

개인정보 상담 사례를 통한 Q&A

Q 대학교 홈페이지에서 비밀번호 찾기를 하면 화면에서 저의 비밀번호를 그대로 보여줍니다. 임시 비밀번호를 부여하는 다른 사이트와 비교해 볼 때 뭔가 엉성해 보이는 것 같네요.

A 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 합니다.

개인정보처리자는 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치를 취하여 합니다. 이 중에서 비밀번호는 암호화하여 저장하여야 하고, 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 합니다.

구체적으로 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서, 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인하는 것입니다.

따라서 이 사례에서 비밀번호를 그대로 보여 주는 것은 원본 값을 유추하거나 복호화 할 수 없도록 한 일방향 암호화에 해당되지 않습니다.

Q 사이버 대학교 사이트를 회원 로그인을 하는데 패킷 분석 프로그램을 통해 확인해 보니 기입한 비밀번호가 전송과정에서 암호화가 되지 않고 그대로 보여 집니다.

A 비밀번호는 정보통신망을 통해 송신하는 경우 암호화하여야 합니다.

개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장 매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 합니다.

비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않아야 하는 중요한 정보입니다. 만약 비밀번호가 암호화되지 않으면 인터넷에서 구할 수 있는 패킷 분석프로그램 등을 통해 쉽게 비밀번호를 확인할 수 있습니다.

따라서 정보통신망을 통하여 비밀번호를 송신하는 경우에는 SSL* 등의 통신 암호 프로토콜이 탑재된 기술을 활용하여 암호화하여야 합니다.

개인정보 범위

등급	등급설명	분류	대상 개인정보
1등급	그 자체로 개인의 식별이 가능하거나 배우 민감한 개인정보 또는 관련 법령에 따라 처리가 엄격하게 제한된 개인정보	고유식별정보	• 주민등록번호, 여권번호, 운전면허번호, 외국인 등록번호 ※ 개인정보보호법 제24조 및 동법 시행령 제19조
		민감정보	• 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 병력(病歷), 신체적·정신적 장애, 성적(性的) 취향, 유전자 검사 정보, 범죄 경력정보 등 사생활을 현저하게 침해할 수 있는 정보 ※ 개인정보보호법 제23조 및 동법 시행령 제18조
		인증 정보	• 비밀번호, 바이오정보(홍채, 지문, 정맥 등) ※ 개인정보의 안전성 확보조치 기준 고시 제7조
		신용정보/금융정보	• 신용점보, 신용카드번호, 계좌번호 등 ※ 신용정보의 이용 및 보호에 관한 법률 제2조, 제19조 및 동법 시행령 제2조, 제16조, 제21조, 별표2 등 ※ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조제4항제2호 및 관련 고시(개인정보의 기술적·관리적 보호조치 기준) 제6조제2항
		의료 정보	• 건강상태, 진료기록 등 ※ 의료법 제22조, 제23조 및 동법 시행규칙 제14조 등
		위치정보	• 개인 위치정보 등 ※ 위치정보의 보호 및 이용에 관한 법률 제2조, 제16조 등
2등급	조합되면 명확히 개인의 식별이 가능한 정보	개인 식별 정보	• 이름, 주소, 전화번호, 핸드폰번호, 이메일주소, 생년월일, 성별 등
		개인 관련 정보	• 학력, 직업, 키, 몸무게, 혼인여부, 가족상황, 취미 등
3등급	개인식별정보와 조합되면 부가적인 정보를 제공하는 간접 개인정보	자동생성정보	• IP주소, MAC주소, 사이트 방문기록, 쿠키 등
		가공정보	• 통계성 정보, 가입자 성향 등
		제한적 본인식별정보	• 회원번호, 사번, 내부용 개인식별정보 등

출처: KISA

감사합니다

당신에게 좋은보험 삼성화재