한국대학교육협의회
Korean Council for University Education

2026년

대학정보공시와 개인정보보호

2026. 03. 18.

정보보호 및 개인정보보호 관련 문의
E. ssjeong99@naver.com

강사 정 상 섭

강사 소개

프 로 필

- (현) 동국대학교 국제정보보호대학원 겸임 교수
- (현) 개인정보보호 교육 전문강사(개인정보보호위원회)
- (현) 정보보호 교육강사(한국정보보호산업협회)
- (현) 개인정보 영향평가(KCA, 한국전산감리원), ISMS-P 인증심사원
- (현) 비에스정보기술 기술연구소 상무
- (전) IBK기업은행 정보보호 팀장

강사 정 상 섭

주요경력

- 전산센터 이전 및 종합정보통신망 구축
- IBK 정보보호 정책기획 및 전략연구
- IBK ISMS-P, ISO27001, 개인정보 영향평가
- 정부, 공공기관, 대학 등 개인정보 영향평가 수행

자격증

- PIA(개인정보 영향 평가 전문인력)
- ISMS-P 인증심사원, ISO27001 심사원
- CPPG(개인정보관리사), 정보시스템 감리원
- 네트워크관리사, 해킹보안전문가, 가명정보전문가
- 사이버보안융합전문가 등

문의 이메일주소 : ssjeong99@naver.com 전화 : 010-8130-1001

목 차

한국대학교육협의회
Korean Council for University Education

CONTENTS

Ⅰ. 개인정보 기본 이해

❖ 우리가 잘 못 이해하는 개인정보 용어들...

개인 정보

제2조(정의)

개인정보란? 살아 있는 개인에 관한 정보로

- 성명, 주민등록번호, 영상 등 개인을 알아볼 수 있는 정보
- 가명정보란? **가명처리**를 하여 추가정보 없이 개인을 알아볼 수 없는 정보
  - 가명처리란? 개인정보를 일부 삭제하거나, 대체하여 개인을 알아볼 수 없도록 처리

➡ 가명처리한 가명정보도 개인정보 해당 할까요?

가명정보도 법에서는 명확하게 개인정보로 명시

망자의 주민등록번호도 개인정보에 해당 할까요?
망자의 정보는 개인정보에 해당하지 않습니다

개인 정보 파일

일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물

➡ 수기로 작성한 파일도 체계적으로 배열만 한다면 개인정보 파일에 해당 할까요?

수기로 성명, 전화번호, 주소 등을 체계적으로 관리 한다면 개인정보 파일에 해당

개인정보 처리자

업무를 목적으로 개인정보파일을 운용하거나, 처리하는 공공기관, 법인, 단체 및 개인

➡ 공공기관의 개인정보처리자는 누구일까요?
기관장님일까요? 아니면 개인정보 보호책임자(CPO)일까요?
그것도 아니면 개인정보취급자 일까요?

개인정보처리자는 그 누구도 아닌 공공기관 자체가 개인정보처리자입니다

Ⅰ. 개인정보 기본 이해

❖ 우리가 잘 못 이해하는 개인정보 용어들...

개인정보 처리시스템

개인정보를 처리할 수 있도록 체계적으로 구성한 시스템

- 전산장비, 프로그램, DB, 서버, 네트워크 등이 해당

접속기록

접속기록은 누가, 언제, 어디서, 무엇을 했는지를 빠짐없이 알수 있도록

계정, 접속**일**시, **접**속지 정보, **수**행업무, **처**리한 정보주체 정보를 반드시 기록 -> 법에 명시

고유식별 정보

주민등록번호
여권번호
운전면허번호
외국인등록번호

민감정보

노동조합 또는 정당가입
사상이나 신념
정치적 견해
유전정보
범죄경력
건강
성생활
생체인식정보
인종
민족

저소득정보가 민감정보에 해당 할까요?

일반 소득정보에 해당

Ⅰ. 개인정보 기본 이해

❖ 우리가 잘 못 이해하는 개인정보 용어들...

인증정보

로그인 등에서 이용자의 **신원을 확인** 하는데 사용하는 정보

- 비밀번호, 인증서, OTP
- 생체인식정보
- 일회용 인증번호

생체인식 정보

생체정보 중 특정한 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리한 정보

- 얼굴, 지문, 홍채, 음성 인식

정보주체

개인정보의 주인

- 이름, 전화번호, 주소
- CCTV에 촬영된 사람
- 응시자, 민원인, 환자 등

이용자

서비스나 시스템을 이용하는 사람

- 홈페이지 또는 시스템을 이용하는 사람
- 개인정보를 입력하거나 조회하는 사람
- 직원, 관리자, 사용자 등

정보주체는 '**내 정보의 주인**', 이용자는 '**서비스를 이용하는 사람**' 입니다

❖ 개인정보의 주요 유형 및 관리 방안

1. 인적사항 : 성명, 주민등록번호, 주소, 전화번호, 이메일 등
① 공개 시 원칙적으로 동의 또는 법적 근거가 필요
② 전화번호, 주소 등을 공개할 경우 마스킹 처리 후 공개

2. 신체정보 : 사진, 영상(CCTV), 지문, 유전자, 건강 상태 등
① 공개 전에 정보주체의 명확한 동의 여부를 확인
② 공개할 때는 모자이크 또는 가리기 등을 적용하여 공개

3. 학적정보 : 학번, 학과, 학년, 수강 과목, 성적, 징계 이력 등
① 개인을 식별할 수 있는 정보로 공개에 특히 신중해야 하며,
② 공개가 필요한 경우에는 통계 처리나 비식별 조치하여 공개

4. 재산정보 : 급여, 장학금, 학자금 대출, 연구비 내역, 기부금 등
① 원칙적으로 공시 대상이 아니며,
② 법령에 따라 공개하는 경우, 필요한 최소범위만 공개하고, 비식별 또는 익명화 조치해야 함

5. 기타 식별정보 : 차량번호, 계좌번호, IP 주소, 출입 기록 등
① 다른 정보와 결합할 경우 개인 식별 가능성이 있으므로, 외부 공개는 엄격히 제한
② 공개가 필요한 경우에는 부분 마스킹 등 비식별 조치를 해야 함

❖ 대학에서의 개인정보

1. **대학정보 공시항목은 통계데이터, 기관정보, 교육과정정보, 재정정보 등으로 개인정보를 포함하지 않습니다.**

2. 다만, PDF 첨부파일에서 개인정보가 노출될 가능성이 있으므로, 철저한 검토가 필요합니다.

① **PDF 파일 :** 성명, 연락처, 주소 등
✓ 개인정보는 동의 없이 공개하면 안됨

② **규정집 PDF :** 특정 개인의 징계/포상 내역 (학번, 성명) 등
✓ 개인을 식별할 수 있는 정보는 삭제하거나 비식별 처리 후 공개

③ **위원회 관련 문서 :** 외부 위원의 연락처, 주민등록번호, 계좌 정보, 서명 등
✓ 소속·직위 외 정보는 비공개하고, 필요 시 마스킹 또는 동의를 확인 후 공개

④ **증빙 서류 스캔본 :** 주민등록번호, 계좌번호, 주소, 연락처, 신분증 사본 등
✓ 개인을 식별할 수 있는 경우, 개인정보는 마스킹 처리하고, 신분증 사본과 고유식별정보는 비공개 해야 함

❖ 개인정보 수집·이용·파기 원칙

① 수집 원칙
- 목적을 분명히 하고 동의
- 필요한 정보만 최소한으로 수집

② 이용 원칙
- 수집 목적 외 이용 금지
- 안전하게 관리하고 비식별화 조치

③ 파기 원칙
- 보유기간이 지나면 개인정보를 지체 없이 파기
- 파기할 때는 복구할 수 없는 방법을 사용
- 정기적으로 파기 여부를 점검하고 관리

1. 개인정보 수집 원칙

① 목적 명확화
- 개인정보를 수집하기 전에 목적을 명확히 해야 하며,
- 무엇 때문에 수집하는지 정보주체에게 분명하게 알려야 함.

② 최소 수집
- 개인정보는 업무 목적을 이루는 데 필요한 만큼만 받아야 하며,
- 많이 받을수록 좋은 것이 아니라, 꼭 필요한 정보만 받는 것이 원칙.

③ 동의 또는 법적 근거
- 원칙적으로 본인의 명확한 동의가 필요하며,
- 동의 없이 수집하려면 법적 근거가 있어야 함.

❖ 개인정보 수집·이용·파기 원칙

2. 목적외 이용·제공 금지 원칙

◆ 허용되는 경우

① 정보주체의 별도 동의가 있는 경우

② 다른 법률에 특별한 규정이 있는 경우

③ 급박한 생명, 신체, 재산의 이익을 위해 필요한 경우

◆ 금지되는 경우

① 수집 목적과 다른 용도로 이용하는 경우

② 동의 없이 제3자에게 제공하는 경우

③ 업무 목적 없이 임의로 조회하는 경우

④ 개인적 호기심으로 열람하는 경우

◆ 위반 시

- 과태료 부과, 형사처벌, 손해배상 책임, 징계, 기관 신뢰도 하락으로 이어질 수 있음

❖ 공시 담당자 주의사항

- 공시가 완료된 데이터는 지체 없이(5일 이내)에 파기해야 하며, 다른 부서에 제공해서는 안 됩니다

❖ 개인정보 수집·이용·파기 원칙

3. 개인정보 파기 원칙

개인정보는 이용 목적 달성 후 지체 없이(5일 이내)에 파기해야 합니다.

◆ 개인정보 파기 시점

① 보유기간이 지난 경우
② 처리 목적을 달성한 경우
③ 동의가 철회된 경우

◆ 개인정보 파기 방법

① 종이 문서는 파쇄하거나 소각
② 전자파일은 복구할 수 없도록 영구 삭제
③ 데이터베이스 기록은 해당 정보를 삭제하고 복구되지 않도록 조치

4. 공시 담당자의 개인정보 파기 원칙

① 공시가 끝난 내부 업무용 파일은 바로 삭제.
② 개인정보가 들어 있는 이메일 첨부파일은 영구 삭제.
③ 임시 폴더 등 저장 위치는 정기적으로 확인하고, 불필요한 파일은 파기.
④ 이동식 저장매체의 데이터도 안전한 방법으로 삭제.

목 차

한국대학교육협의회
Korean Council for University Education

CONTENTS

Ⅱ. 유출 발생 시 대응

1. 개인정보 유출이란?

- 법령이나 개인정보처리자의 자유로운 의사와 관계없이, 개인정보가 **외부에 공개되거나 제3자가 접근 가능한 상태**를 개인정보 유출이라고 합니다.

2. 개인정보 유출과 노출의 차이

◆ 유출 (Leakage)

개인정보가 정보주체의 의도나 법적 근거 없이 **정보가 실제로 제3자에게 넘어간 상태**

➢ **주요 특징:**

① 해킹으로 데이터베이스가 탈취
② 개인정보가 저장된 USB를 분실
③ 이메일 오발송으로 다른 사람에게 전달

◆ 노출 (Exposure)

개인정보가 정보주체의 의도와 관계없이 **외부에서 누구나 접근 가능한 상태**

➢ **주요 특징:**

① 홈페이지에 개인정보 포함 문서 게시
② 공개 게시판에 PDF 파일 첨부
③ 누구나 접근가능한 클라우드에 파일 저장

◆ 유출이나 노출이 의심되면 즉시 보고해야 합니다.

- 두 경우 모두 개인정보 사고로 이어질 수 있으므로, 내부 절차에 따라 신속히 통지·신고 여부를 확인해야 합니다.

Ⅱ. 유출 발생 시 대응

3. 유출 시 통지 의무

- 개인정보 유출을 알게 된 경우에는 **지체없이(72시간 이내)**에 정보주체에게 관련 사항을 통지해야 합니다.

① 유출된 개인정보 항목

- 이름, 전화번호, 이메일 주소 등 유출된 항목을 구체적으로 명시하고,
- '일부 개인정보'와 같은 모호한 표현은 사용하지 않아야 함.

② 유출 시점과 경위

- 유출이 발생한 날짜와 시간 등 시점을 정확히 밝혀야 하며,
- 해킹, 시스템 오류, 직원 실수 등 유출 원인과 경위를 구체적으로 설명.

③ 피해 최소화 방법

- 비밀번호 변경, 명의 도용방지 서비스 신청 등 필요한 조치를 안내해야 하며,
- 정보주체가 바로 실천할 수 있는 구체적인 대응 방법을 알려야 함.

④ 대응 조치 및 연락처

- 보안 강화, 수사기관 신고 등 개인정보처리자의 조치 사항을 안내하고,
- 피해 접수 및 상담을 위한 담당 부서와 연락처를 제공.

❖ 72시간 내 통지 의무

① 개인정보 유출을 알게 되면 지체없이 72시간 이내에 통지.
② 통지 기준은 유출이 최종 확인된 시점이 아니라, 유출 사실을 알게 된 시점.
③ 통지나 신고가 늦어지면 과태료 등 법적 책임과 기관 신뢰도 하락으로 이어질 수 있음

목 차

한국대학교육협의회
Korean Council for University Education

CONTENTS

Ⅲ. 대학의 노출 사례 및 예방

1. 사례 : 엑셀 파일의 숨겨진 시트

➢ 사건 개요

1. 문제 발생

- C대학교가 통계 자료를 공개하는 과정에서,
- **엑셀의 숨겨진 시트**에 학생 500명의 개인정보가 함께 **공개**.

2. 유출 원인

- 엑셀의 시트 숨기기는 보안 조치가 아니며,
- 원본 데이터를 그대로 사용한 것이 유출원인

3. 대응 및 제재

- 유출 파일은 삭제 후 개인정보를 제거하여 수정본을 재 업로드
- 학생 500명에게 개별 통지하고, 개인정보 보호위원회에 신고
- 그 결과 과태료 500만원과 재발방지 교육 명령이 부과

➢ 올바른 처리 방법

1. 개인정보가 포함된 원본 엑셀 파일은 **공시용으로 사용 금지**
2. 공시용 파일은 **빈 엑셀 파일을 새로 만들어 작성**
3. 원본에서는 필요한 데이터만 **"선택해 값으로 붙여넣기로 복사"**
4. 숨기기 취소 메뉴에서 **숨겨진 시트가 없는지 점검**
5. 자료에 불필요한 수식이나 외부 참조가 남아 있는지 점검 후 제거.
6. 개인정보가 모두 제거되었는지 최종 확인한 뒤, 원본과 구별되는 이름으로 저장.

❖ 복사·붙여넣기 시 주의사항

- 숨겨진 행이나 열에도 개인정보가 남아 있을 수 있으니 주의해야 하고,
- **복사할 때는 반드시 '값 붙여넣기'를 사용**한 후, 개인정보 포함 여부를 다시 확인 해야함.

Ⅳ. 실무 점검 가이드

2. 파일(HWP, Word, Excel)에 숨겨진 개인정보 제거 방법

1. 한글/HWP 파일

1. 원본 문서 열기
- 한글(HWP) 파일을 열고
- Ctrl+F로 성명, 연락처, 주민등록번호, 주소등 개인정보를 검색

2. 개인정보 삭제/마스킹
- 개인정보는 삭제하거나, *** 등으로 마스킹
- 서명은 이미지나 자필이 남지 않도록 처리

3. PDF 변환 및 확인
- 파일을 PDF로 변환한 뒤, PDF 전체 페이지에, 개인정보가 남아 있는지 재점검

4. 파일 정보 점검
- PDF의 제목, 작성자 등도 함께 확인 및 정리

2. MS Word 파일

1. 문서 검사 실행 방법
- 파일 → 정보 → 문제 확인 → 문서 검사를 순서대로 실행하여 숨겨진 개인정보를 검출

2. 검출 항목 제거
- 검사 결과에서 모두 제거를 클릭
- 개인정보를 일괄 삭제

3. 본문 수동 확인
- 검토탭에서 누락된 개인정보를 확인
- Ctrl+F로 본문 검색 및 수정/삭제

4. PDF 변환 및 최종 확인
- 다른 이름으로 저장 → PDF로 변환
- PDF에서 개인정보가 남아 있는지 다시 확인

3. 엑셀 파일

1. 필수 점검 사항

① 시트 탭을 우클릭하여 **숨기기 취소**로 숨김 시트가 있는지 확인
② 행/열 번호가 건너뛰는지 확인하여 숨김 여부 점검
③ 셀 메모, 댓글에 개인정보가 남아 있는지 확인

2. **권장 방법**
- 외부 제공용은 **새 파일을 만든 뒤, 필요한 데이터만 "값 붙여넣기"** 해서 저장해야 함

목 차

한국대학교육협의회
Korean Council for University Education

CONTENTS

Ⅴ. 개인정보보호 인식제고

1. 개인정보취급자의 책임

❖ 자료를 공시할 때는 개인정보가 포함되어 있거나 노출될 가능성이 없는지 반드시 확인해야 합니다.

① **인식 전환**
개인정보는 누구나 실수로 노출할 수 있으므로 모든 업무 과정에서 항상 주의가 필요

② **예방적 점검**
공시 자료에는 개인정보가 포함될 수 있으므로, 공개 전에 반드시 확인

③ **즉시 대응**
개인정보가 노출된 사실을 알게 되면 지체 없이 보고하고 즉시 대응.

2. 개인정보보호 5대 실천 수칙

① **파일 분리 관리 :** 내부용 파일과 공시용 파일은 구분하여 별도로 관리
② **업로드 전 전수 점검 :** 첨부파일을 업로드하기 전에 전체 내용을 반드시 확인
③ **마스킹 습관화 :** 개인정보가 포함된 문서는 마스킹 처리한 후 첨부
④ **동료 교차 검증 :** 중요한 자료는 동료와 함께 한 번 더 확인
⑤ **즉시 보고 :** 개인정보 노출을 발견하면 지체 없이 바로 보고

3. 자주 묻는 질문 (FAQ)

Q1. 통계 데이터를 공시할 때 주의할 사항은 무엇인가요?

통계 데이터는 개인정보가 아닐 수 있으나, 첨부파일의 개인정보 포함 여부는 반드시 확인해야 합니다.

Q2. 공시된 파일에서 개인정보가 발견되면 어떻게 해야 하나요?

개인정보가 발견되면 파일을 즉시 삭제 또는 비공개 처리하고, 담당자에게 바로 보고해야 합니다. 필요 시 신고 절차도 함께 진행해야 합니다.

4. (참고) 핵심 요약

① 통계 데이터를 공시할 때는 원본 파일에 개인정보가 포함되어 있는지 반드시 확인

② 개인정보가 발견되면 해당 파일을 즉시 삭제하거나 비공개 처리하고, 담당자에게 바로 보고

목 차

한국대학교육협의회
Korean Council for University Education

CONTENTS

Ⅴ. 공시담당자의 개인정보보호 실천지침

01 개인정보 취급 기본 원칙

① **최소 수집**
업무에 꼭 필요한 개인정보만 **최소한으로 수집**.

② **명확한 목적**
수집 목적을 분명히 하고, 동의 받은 **범위 내에서만 사용**.

③ **안전한 관리**
개인정보는 반드시 **암호화하여 저장**하고, **접근 권한 있는** 사람만 열람.

④ **정확성 및 최신성**
항상 **정확하고 최신 상태로 관리**하며, 오류 시 즉시 수정.

⑤ **파기 원칙**
보유기간이 끝나거나 목적이 달성되면, **지체 없이(5일) 안전하게 파기.**

02

PC 및 정보 시스템 보안

공시담당 실천 지침

① **강력한 비밀번호 사용**
비밀번호는 영문 대/소문자, 숫자, 특수문자를 조합해 **9자리 이상**으로 설정하고
3개월마다 변경

② **화면 잠금 습관화**
자리를 비울 때는 **Win + L**로 화면을 잠그고, 퇴근 시에는 반드시 **PC 전원을 종료**

③ **보안 프로그램 관리**
백신 프로그램은 **최신의 상태를 유지**, 소프트웨어는 **정품만 사용**

④ **의심스러운 메일/링크 주의**
모르는 발신자의 **이메일·SMS·링크는 절대 클릭하지 말고, 의심스러운**
첨부파일은 정보보호팀 확인 후 실행

⑤ **계정 분리 사용**
공용계정은 사용하지 말고 개인별 계정으로 로그인하고,
업무용과 개인용 계정은 분리하여 사용

03 문서 및 자료 관리

① **종이 문서 파쇄**
개인정보가 포함된 종이문서는 업무 종료 후 **반드시 파쇄**.
파쇄기가 없을 경우 **잠금장치**가 있는 장소에 **보관** 후, 주기적으로 **전문 업체**에 위탁하여 **파쇄**.

② **전자문서 암호화**
개인정보가 담긴 전자문서는 반드시 **암호화하여 저장 및 전송하고,**
문서는 **비밀번호를 설정하여** 관리.

③ **이동식 저장매체 보안**
개인정보가 포함된 **USB는 암호화하여 사용**하고, 사용 후에는 즉시 삭제 또는 안전하게 보관, 업무와 무관한 **개인 USB는 절대 사용 금지**

④ **클라우드/공유 폴더 관리**
클라우드나 공유폴더에 개인정보를 저장할 때에는 **반드시 암호 설정 및 접근권한을 최소화**

04

공시담당 실천 지침

상담 및 정보주체 응대 시 보안

① **본인 확인 철저**
상담 시 반드시 신분증 또는 등록된 연락처 등으로 **본인 확인,**
본인 여부가 불확실 때는 개인정보 **제공 금지**.

② **사생활 보호 및 정보요청 제한**
주변에 고객 정보가 들리지 않도록 **공간을 확보,**
목소리는 크기를 조절하고, 불필요한 **개인정보는 절대로 요구하면 안됩니다.**

③ **동의 없는 정보 공유 금지**
정보주체의 동의 없이 개인정보나 상담 내용을 제3자에게 **공유하면 안되고,**
업무상 공유가 꼭 필요한 경우 **비 식별화 원칙을** 준수하고,
SNS 등 외부 매체에 **개인정보와 관련된 언급은 절대 금지 입니다**.

05

공시담당 실천 지침

개인정보 유출 사고 발생 시 대응 절차

신속하고 정확한 초기 대응 중요

자체 은폐 시 가중 처벌

① **즉시 보고**
유출 사실을 인지하는 즉시 개인정보 보호책임자(CPO) 또는 상사에게 **즉시보고**

② **유출 확인 및 차단**
유출 경로와 범위를 신속히 **파악하고**, 추가 유출 방지를 위한 **조치 수행**

③ **피해 최소화 조치**
유출된 정보의 **영향도를 파악** 한후 정보주체의 **피해를 최소화 할 수 있도록 조치**

④ **사고 조사 협조**
조사 과정에 적극 협조하고, 사고 발생부터 처리까지 **상세히 기록**

⑤ **대외 공지 및 신고**
일정 규모 이상의 사고는 법에 따라, 개인정보 보호위원회 또는 KISA에 **신고하고,** 정보주체에게 **통지**

06

개인정보 보호법 주요 개정 및 처벌 규정

❖ 개인정보보 보호법

1. 2011년 9월 30일 : 처음 시행

2. 20년 9월 15일 : 1차 전면 개정
- **감독체계를** 개인정보 보호위원회로 **일원화**

3. 23년 9월 15일 : 2차 전면 개정
- 온라인과 오프라인 **규제를 통합**

4. 26년 3월 10일 : 주요 개정
- **과징금을 전체 매출액 3% → 10%로 상향**

❖ 처벌 규정

- **관리 소홀로 개인정보가 유출될 경우**
  - 기관 : 과징금 부과 등 법적 책임이 따를 수 있음.
  - 기관장 및 직원 : 관련 규정에 따라 징계 조치를 받을 수 있음.

개인정보보호, 우리 모두의 책임입니다.

개인정보보호는 한 사람의 노력이 아닌,
모든 임직원이 함께 지켜야 할 중요한 가치입니다.

인 식	실 천	보 고
개인정보보호의 중요성을 항상 인식	일상 업무에서 보안 수칙을 철저히 준수	의심스러운 활동은 즉시 보고

감사합니다