2026년 상반기 개인정보 처리 유의사항 안내

<정보보호팀, 2026. 2. 27.>

❖ **신학기 개인정보 수집·이용 집중 시기**에 **불필요한 개인정보 수집 방지** 및 **이메일, 메신저 등을 통한 개인정보 유출 예방**을 위해 다음의 **개인정보 처리 유의사항**을 안내함

1 업무 처리 시 유의해야 할 개인정보 처리

1. 개인정보처리시스템, 홈페이지 등에서의 개인정보 처리

「참고」 개인정보 유출 사례

☞ 반 편성 정보를 알리는 과정에서 **불필요한 개인정보**(성적 등)**가 포함된 자료 게시**

☞ 정보공개청구에 따라 제공한 파일에 **엑셀의 다양한 기능**(숨기기, 개체 삽입 등)이 적용되어 **숨겨진 개인정보 발견**

☞ 전출된 직원의 **접근권한을 말소하지 않아** 해당 직원이 업무시스템에 접속하여 **개인정보 유출**

○ **강당·벽면·교내 게시판용 자료** 및 **홈페이지 업로드용 파일 내**에 **개인정보 포함되지 않도록 반드시 확인**

○ 홈페이지에 **엑셀문서 게시 지양**(☞ PDF 변환 게시)

※ 부득이하게 엑셀파일 탑재 시 비밀번호를 설정하고 숨기기 처리된 행·열* 사전 확인 필수

* Excel 암호설정 : 파일 → 정보 → 통합 문서 보호 → 암호 설정
* 숨긴 행·열 표시 : Ctrl + A(전체선택) → Ctrl + Shift + 9(행) / Ctrl + Shift + 0(열)
* 숨긴 메모 표시 : 검토 → 메모표시 ☞ 개인정보가 포함된 메모 삭제

※ **엑셀 외부링크 연결** 기능으로 다른 파일의 개인정보가 포함될 가능성이 있어 **점검·삭제** 필요

○ 개인정보처리시스템* 및 개인정보 처리 업무와 관련된 **접근권한**은 법령 또는 업무규정 등에 따라 **업무수행**에 **필요한 최소한의 범위**로 **부여**

* 나이스, 에듀파인, 학사관리시스템 등

※ 권한없는 자(사회복무요원 등)에게 접근권한 임의로 양도 또는 대여 금지

○ **클라우드 스토리지***(구글 드라이브, 드롭박스 등)에 학생, 교직원 등의 **개인정보**가 포함된 자료를 **업로드**하지 않도록 **유의**

* 클라우드 스토리지란? 인터넷(네트워크 기반)을 통해 데이터를 저장, 관리 할 수 있는 공간

2. 이메일, 메신저, 공문에서의 개인정보 처리

「참고」 개인정보 유출 사례

☞ 성적, 졸업 관련 정보가 포함된 이메일 발송 시, 당사자 외의 **타인의 개인정보를 포함하여 발송**

☞ 개인정보취급자가 개인정보가 포함된 파일을 **이메일을 통하여 다수의 사용자에게 무분별하게 발송**

☞ SNS **단체 대화방, 메신저** 등을 통해 교직원이 다수 학생에게 공지사항을 안내하며 개인정보 포함된 자료를 공유

☞ 합격결과 통보, 학사일정 안내, 교육프로그램 홍보 등을 다수의 학생에게 **집단메일로 발송**하여 타인의 **이메일 정보 노출**(☞**개별발송 기능 사용**)

❍ **이메일**을 이용하여 개인정보가 포함된 파일을 전송할 경우, **메일 수신자(개인·단체) 및 파일 암호설정 여부** 반드시 확인

❍ 실시간 정보공유가 가능한 **기관 메신저** 등을 이용하여 업무정보를 주고받는 경우, **개인정보 탑재 지양**

❍ **공문**(붙임파일 포함)에 **개인정보가 포함**된 경우, **문서보안(보안 결재), 열람범위 지정, 열람제한** 등의 기능을 활용하여 개인정보 유·노출 주의

3. 생성형AI 사용 시 개인정보 처리

❍ 학생·교직원 등의 **개인정보·민감정보**를 **생성형AI 입력창**(프롬포트)에 입력되지 않도록 하고 필요시 개인을 특정할 수 없도록 비식별화 사용

※ 챗GPT와 같은 생성형AI에 개인정보·민감정보 입력 시 해당 AI의 학습에 재이용되어 타인에게 결과물(개인정보·민감정보 포함) 노출 위험 발생

❍ 생성형AI 사용 전 관련 법령* 및 안내서** 사전 확인 필요

* 개인정보보호법 제15조(개인정보의 수집·이용), 제17조(개인정보의 제공), 제18조(개인정보의 목적 외 이용·제공 제한), 제23조(민감정보 처리 제한) 등

** 생성형 AI 개발·활용을 위한 개인정보 처리 안내서('25.8.)(개인정보보호위원회), 국가·공공기관 AI보안 가이드북('25.12.)(국가정보원)

2 업무 처리 시 숙지해야 할 주요 개인정보 보호법(이하 '법')

1. 개인정보 수집·이용 및 수집 제한 「법 제15조, 제16조, 제22조의2」

「참고」 법 위반 사례
☞ **(최소수집 위반)** 학사업무와 무관한 학부모의 직업, 학력, 생년월일 등 개인정보를 **과도하게 수집**하는 사례

○ 정보주체의 동의, 법령상 의무 준수, 공공기관의 소관 업무 수행 등을 위해 개인정보 수집·이용 가능

○ 개인정보의 **①수집·이용 목적, ②수집 항목, ③보유 및 이용 기간, ④동의 거부권과 그에 따른 불이익 내용 고지 후 동의**

※ 수집 시 준수사항은 「각급학교 개인정보 수집업무 길잡이」('24.2) 참고 (교육부 개인정보보호 포털)

○ 개인정보는 처리 목적에 따라 **필요한 최소한의 정보만 수집**하고, 목적에 맞는 용도로 활용

※ 업무처리 과정에서 얻은 개인정보를 이용하여 법령에서 금지하는 행위를 하는 경우 처벌될 수 있음을 유의

○ **만 14세 미만 아동의 개인정보 처리의 경우,** ①법정대리인의 **동의,** ②법정대리인의 **동의여부 확인,** ③만 14세 미만의 아동에게 **이해하기 쉬운 양식과 명확하고 알기 쉬운 언어로 안내**

2. 개인정보 제3자 제공·위탁 「법 제17조, 제18조, 제26조」

「참고」 법 위반 사례
☞ **학사업무**를 **목적**으로 수집한 학생의 개인정보를 **홍보·마케팅 등** 수집 목적 범위를 초과하여 이용하거나 **제3자에게 제공**
☞ **민원업무로 알게 된** 민원인의 성명, 연락처 등의 **개인정보를** 정당한 이유 없이 **피민원기관에 제공**
☞ 민원인이 선생님의 핸드폰번호를 요구하여, **해당 선생님의 동의 없이 핸드폰번호 제공**
☞ 총동창회에서 학교에 졸업생의 성명과 연락처, 졸업 연도가 기재된 졸업생 명부를 달라고 요구하여, **학교에서 졸업생들의 동의를 구하지 않고 이를 임의로 제공**

○ 개인정보를 **목적 내** 또는 **목적 외 이용·제공**할 경우 제공받는 자는 **개인정보 안전성 확보 조치 마련**

- (**목적 내**) 정보주체 동의*, 타 법률에 규정, 공공기관 소관 업무 수행 등의 경우 **수집목적의 범위 내에서** 제3자 제공 가능

* (**동의 시 고지사항**) ①제공받는 자, ②제공받는 자의 이용 목적, ③제공 항목, ④제공받는 자의 보유 및 이용 기간, ⑤동의 거부권 및 그에 따른 불이익 내용

- (**목적 외**) 정보주체 동의, 타 법률에 규정(국정감사 등), 범죄 수사, 법원 재판 등의 경우 **수집목적 외의 용도로** 제3자 제공 가능

※ 제3자에게 제공한 날로부터 30일 이내, 10일 이상 홈페이지 또는 관보 등에 게재*

* (**게재할 내용**) ①목적외이용등을 한 날짜, ②법적 근거, ③목적, ④개인정보의 항목(구성)

○ 개인정보처리 위탁 시 **문서(표준 개인정보처리위탁 계약서)**로 계약을 체결하고, 홈페이지 **개인정보 처리방침**에 포함하여 **공개**

※ 수탁자가 재위탁시 위탁자의 **동의 필수**, 재위탁받은 수탁자도 **개인정보처리방침**에 **공개**

※ 수학여행, 졸업앨범 제작 등을 위한 업무 위탁 시 **수탁자 관리·감독 철저**

3. 고정형 영상정보처리기기(CCTV 등) 설치 · 운영 「법 제25조」

「참고」 법 위반 사례
☞ (**과태료 처분**) 00고등학교 **화장실**에 학생 흡연 및 학교 폭력 방지를 위한 목적으로 고정형 영상정보처리기기(CCTV) **설치**

○ (**공개된 장소**) 공개된 장소에서의 고정형 영상정보처리기기 설치는 **원칙적**으로 **금지**되고 예외적으로 **개인정보 보호법 제25조에서 정하는 사유에 해당하는 경우에만** 고정형 영상정보처리기기 **설치·운영** 가능

【 고정형 영상정보처리기기 설치·운영 허용 】

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설의 안전 및 화재 예방을 위하여 정당한 권한을 가진 자가 설치 운영 한 경우
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치 운영 한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치 운영 한 경우
6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우
   가. 출입자 수, 성별, 연령대 등 통계값 또는 통계적 특성값 산출을 위해 촬영된 영상정보를 일시적으로 처리하는 경우
   나. 그 밖에 이에 준하는 경우로서 보호위원회의 심의 · 의결을 거친 경우

※ 정당한 권한 없이 임의로 CCTV를 설치하여 공개된 장소를 촬영하는 행위 금지

- 단, 불특정 다수가 이용하여 **현저히 사생활 침해 우려가 있는 장소 (목욕실, 화장실, 발한실, 탈의실 등)**는 **고정형 영상정보처리기기 설치·운영 금지**

※ [참고] "공개된 장소" 예시
☞ 누구나 출입, 접근 또는 통행이 허용되는 장소(학교 운동장, 학교 복도* 등)
* 다만, 학교 건물이 엄격하게 출입통제 및 관리되는 경우 비공개 장소로 볼 수 있음

○ **(비공개된 장소)** 비공개 장소에 업무를 목적으로 고정형 영상정보처리기기를 설치하는 경우에는 **법 제15조**(개인정보의 수집 · 이용)에 따라 설치·운영 가능

※ [참고] "비공개된 장소" 예시
☞ 학생, 교사 등 학교 관계자만 출입이 가능한 학교시설(교실, 실험실 등)

○ **(안내판 설치)** 고정형 영상정보처리기기 운영자는 다음의 **필수사항**이 모두 **포함된 안내판 설치** 필요

안내판 필수사항

① 설치 목적 및 장소
② 촬영 범위 및 시간
③ 관리책임자의 연락처
④ 고정형 영상정보처리기기 설치·운영 사무 위탁하는 경우, 수탁자의 명칭 및 연락처

○ **(열람 등 요구 절차) "10일 이내" 처리 필요**

①열람대상
1. 정보주체
2. 명백히 정보주체의 급박한 생명,신체, 재산의 이익을 위해 필요한 경우

⇒

②열람 등의 청구
정보주체의 개인영상정보 열람 또는 존재확인 요청

⇒

③본인 또는 정당한 대리인 여부 확인

⇒

④열람 여부 결정
1. 법률에 따라 제한된 경우
2. 타인의 생명·신체를 해하거나 재산 등을 침해할 우려가 있는 경우
3. 다음에 해당하는 업무 수행 시 중대한 지장을 초래하는 경우
- 조세의 부과·징수 또는 환급에 관한 업무
- 각급학교, 평생교육시설, 고등교육기관에서의 성적평가 또는 입학자 선발에 관한 업무
- 채용에 관한 시험, 자격심사에 관한 업무
- 보상금·급부금 산정 등에 관한 업무
- 감사 및 조사에 관한 업무

⇒

⑤열람 조치

비식별조치가 가능한 경우	정보주체 외 모자이크 처리
비식별조치가 어려운 경우	타 정보주체의 제3자 제공 동의 징구

⇒

⑥열람 기록·관리
개인영상정보 관리대장 기록 및 관리

4. 개인정보의 처리 제한 「법 제23조, 제24조, 제24조의2」

「참고」 법 위반 사례

☞ **(개인정보 미동의)** 현장학습, 우유급식, 스쿨뱅킹, 졸업앨범 등의 경우 개인정보 수집을 위한 **별도의 법적 근거가 없음**에도 **정보주체의 동의 없이 개인정보를 수집**하는 사례

☞ **(필수 고지사항 누락)** 온라인(홈페이지 등), 오프라인(종이문서) 등을 통해 동의를 받을 때 **4가지 항목* 중 일부 항목만 동의**를 받는 사례

* ①수집 목적, ②수집 항목, ③이용 기간, ④동의 거부권과 그에 따른 불이익 내용

○ **민감정보, 고유식별정보**(주민등록번호 제외) **등의 수집·이용 동의**는 다른 개인정보의 동의와 구분하여 **별도 동의** 필요

○ 주민등록번호는 정보주체의 동의가 있어도 **법률, 시행령에 근거가 없으면 수집 불가**

5. 개인정보 파기 「법 제21조」

「참고」 올바른 개인정보 파기 사례

☞ 개인정보를 포함한 파일은 **처리 목적 달성 시 즉시 파기** 조치

☞ **개인정보가 포함된 인쇄물** 등은 **이면지로 활용해서는 안 되며**, 복원할 수 없도록 파기 처리

☞ **재학생의 사진 등**이 홈페이지 등에 탑재된 경우 별도의 동의가 없다면 **졸업 후에는 반드시 삭제** 처리

○ 개인정보의 **보유기간 경과, 처리목적 등을 달성**한 경우, 별도의 보관 기간이 규정되어 있지 않다면 **지체 없이(5일 이내) 파기**

※ 고정형영상정보처리기기(CCTV) 영상은 특별히 보관기간을 설정하고 있지 않다면 30일 동안 보관 후 파기(표준 개인정보보호지침 제41조)

○ 개인정보 파기는 **절차와 방법에 따라** 기술적, 물리적으로 **복원이 불가능하게 파기**하여야 하며 **파기 후 결과 보고 및 대장 관리**

3 개인정보처리자의 주요업무

○ 기관별 개인정보 관련 변경사항 발생 시 **개인정보파일 (변경)등록, 개인정보 처리방침** 및 **내부관리계획 현행화** 등 추진

○ 개인정보 내부관리계획에 따라 **안전조치의무**(법 제29조, 같은법 시행령 제30조) **이행사항**(붙임)을 **주기적**으로 **철저하게 관리**

- **월 1회 접속기록 점검** 및 **접근권한 부여·관리**
- 개인정보처리 위탁계약 시 **(재)수탁자**의 업무 **관리·감독**
- **안전한 접속수단** 및 **인증수단** 적용, **세션 타임아웃**(Session Timeout)* **설정**, 웹 취약점 점검 및 보완 조치 등 **접근통제 강화**

* 개인정보처리시스템 접속 후 일정시간 업무처리를 하지 않는 경우 자동 접속 차단

- 전산실·자료보관실의 출입통제 철저 및 서류·보조저장매체 등을 안전한 장소에 보관
- 개인정보를 출력(인쇄, 화면표시, 파일생성 등)할 때에는 용도에 따라 **출력 항목**을 **최소화**하고, **출력·복사물**(종이 인쇄물, 외부 저장매체 등)의 안전한 관리를 위한 **안전조치 마련**

※ 공무원이 영리를 목적으로 개인정보를 유출한 사건과 유사한 사례가 발생하지 않도록 개인정보취급자에 대한 접근권한 최소화, 접속기록 점검 등 관리 강화 필요

※ 시험지 유출 사고 등 PC 보안, 출입 통제 미흡에 따른 개인정보 침해사고가 증가함에 따라 접근통제 강화 필요

※ 홈페이지 및 시스템 취약점 점검 등 해킹사고 예방을 위한 안전조치 강화

○ 개인정보 업무담당자, 정보주체 등을 대상으로 **개인정보 보호 교육 실시**

- 개인정보의 보호 인식제고를 위하여 개인정보 보호담당자 및 개인정보취급자에게 정기적(연1회 이상)으로 필요한 교육 실시

※ 교육부 정보보호교육센터(https://sec.keris.or.kr) 개설 교육과정 활용

❍ 개인정보 유출 시 개인정보 유출 등의 통지, 개인정보 유출 신고 및 조치확인서 제출

개인정보 유출의 개념

표준 개인정보 보호지침 제25조(개인정보의 유출등) 개인정보의 분실·도난·유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 **개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것**을 말한다.

- 유출등 통지 방법

구분	내용
통지시기	▶ 유출등 사실을 알게 된 후 **72시간 이내**
통지대상	▶ **정보주체**
통지방법	▶ 서면, 전자우편, FAX전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법 - 단, 정보주체의 연락처를 알 수 없는 경우 인터넷 홈페이지에 통지항목 5개를 30일 이상 게시하는 것으로 정보주체 유출등 통지 의무를 갈음할 수 있음
통지항목	▶ 유출등이 된 개인정보의 항목 ▶ 유출등이 된 시점과 그 경위 ▶ 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 ▶ 개인정보처리자의 대응조치 및 피해 구제절차 ▶ 정보주체의 피해 신고 등을 상담·접수할 수 있는 담당부서 및 연락처

- 유출등 신고 방법

구분	내용
신고시기	▶ 유출등이 되었음을 알게 된 후 **72시간 이내** - 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있음
신고대상	▶ 1명 이상 유출등이 된 경우 상급기관을 경유하여 **교육부**에 신고 ▶ 개인정보가 1천명 이상 유출등이 됐거나, 민감정보·고유식별정보 및 외부로부터의 불법적인 접근에 의해 1건이라도 유출등이 된 경우는 **교육부 및 개인정보위(한국인터넷진흥원)**에 신고
신고방법	▶ 교육부(개인정보보호 포털, privacy.moe.go.kr) 및 개인정보위(개인정보 포털, privacy.go.kr) 홈페이지를 통해 유출등 신고서 제출 - 부득이한 경우 전자우편(moeprivacy@keris.or.kr)을 통해 개인정보 유출 신고서 제출 ▶ 시간적 여유가 없거나 특별한 사정이 있는 경우 상급기관과 교육부에 동시에 신고하며 유출등 신고서 제출
신고내용	▶ 기관명, 유출등이 된 개인정보 항목·규모, 유출등 시점·경위, 유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법, 개인정보처리자의 대응 조치 및 피해 구제절차, 피해 발생 신고 등을 접수할 수 있는 담당부서 및 연락처 등 - 정보주체에 대한 유출등 통지 결과 및 피해 최소화를 위한 긴급 조치 내용이 포함되도록 해야 함
신고양식	▶ 개인정보 유출등 신고서(포털 다운로드)

4 개인정보취급자의 유의사항

- ❍ 업무상 알게 된 개인정보를 정당한 사유 없이 누설하거나 다른 목적으로 이용하지 않도록 **목적 외 개인정보 처리 금지**
- ❍ 개인정보처리시스템 계정은 개인별로 사용하며 타인과 공유하지 않는 등 **비밀번호 관리 철저 및 계정 공유 금지**
- ❍ 개인정보가 포함된 문서, **이동형 저장장치(USB)** 등을 허가 없이 **외부**로 **반출**하거나 **무단 복사 금지**
- ❍ 자리 이탈 시 **PC화면 잠금 설정**
- ❍ 파기해야 할 개인정보문서는 **문서세단기(출력물)를 이용한 파쇄** 또는 **복구가 불가한 기술적 방법을 통한 완전 삭제(전자파일)** 처리
- ❍ 기관이 제공하는 정기적인 **개인정보 보호 교육 이수**

5 기타 참고사항

- ❍ 개인정보보호 업무 관련 자료*는 **교육부 개인정보보호 포털** (https://privacy.moe.go.kr) **참고** (※ 별도 로그인 없이 사용 가능)

  * **자료실> 참고자료**에 개인정보 보호 법령·고시 및 지침 해설서, 업무 사례집, 매뉴얼, 각급학교 개인정보 수집업무 길잡이(표준개인정보파일목록 포함) 등 탑재

- ❍ '개인정보 보호법', '개인정보 보호법 시행령', '교육부 개인정보 보호지침' 등 **관계 법령 및 행정규칙**은 **국가법령정보센터(law.go.kr)**에서 확인 가능

붙임 교육기관 개인정보 안전조치의무(법 제29조) 관련 체크리스트

1. 개인정보 관리 현황

정보주체 건 수	000,000건 (000,000명)
개인정보 파일 수	00개
개인정보처리시스템 수	00식
고유식별정보 보유 현황	□주민등록번호 □여권번호 □외국인등록번호 □운전면허번호
	전체 정보주체 건 수 [000명]
비 고	

□ 개인정보파일 보유 현황

개인정보 파일명(DB명)	정보주체 수 (명)	수집하는 개인정보 항목 ※ 필수/선택 구분	민감정보 및 고유식별정보 수집 여부 ※ 수집시 해당 항목 명시	취급부서	취급자(명)
학사시스템	*5,000,999건 (100,999명)*	*(필수) 학생,연락처 등 (선택) 주소, 건강정보*	*·민감정보(건강) 수집*	*·학적관리팀*	*50*
홈페이지회원 정보	*건수 확인불가 (100,999명)*	*(필수) 이름, 성명, 아이디, 비밀번호 CI (선택) 자택주소*	*·수집하지 않음*	*·인사팀 ·전산팀*	*50*
연구인력관리 시스템	*1.000,999건 (10,999명)*	*(필수) 이름, 성명, , 주소, 이메일주소, 연락처, 주민등록번호*	*·고유식별정보(주민등록 번호) 수집*	*교무팀*	*30*
도서예약정보	*건수 확인불가 5,999,999명*	*(필수) 영문이름, 한글이름, 연락처, 여권번호, 주민번호*	*·고유식별정보(여권정보,주민등록번호) 수집*	*·사서팀*	*30*

□ 개인정보처리시스템 현황

개인정보 처리시스템명	보유개인정보파일명	소프트웨어 아키텍쳐 ※ web, c/s 중 하나 이상 택일	개발업체	유지보수 업체
학사시스템	·학생정보	·web방식	A정보통신	A정보통신
대표홈페이지시스템	·홈페이지회원정보	·web방식	A정보통신	B정보통신
도서예약관리시스템	·홈페이지회원정보 ·회원정보	·web방식, c/s방식	자체개발	자체유지보수

□ 의무대상 파일 개인정보 영향평가 실시 현황

개인정보처리 시스템명	개인정보파 일명	고유식별/ 민감정보	개인정보 보유량	연계시스템 여부	영향평가 실시	비고
학사시스템	·학생정보	건강정보	1,787,070	해당사항 없음	영향평가 실시 2024년 12월 31일	-
대표홈페이지 시스템	·홈페이지 회원정보	주민등록번호	3,244,148	유치원입학관리시스템과 연동	영향평가 실시 2025년 9월 3일 ※ 일부 운영체계 변경으로 2025년도 영향평가 수행	-
도서예약관리 시스템	·홈페이지 회원정보 ·회원정보	주민등록번호 외국인등록 번호	6,999,377	해당사항 없음	영향평가 미실시	2026년도 실시 예정

2. 개인정보처리시스템 자율 점검

개인정보처리시스템에 불법적인 접근 및 침해사고 방지 등을 위해 접근 제한 및 접근통제를 위한 시스템을 구축·운영하거나, 개인정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보호조치를 하여야 한다.(법 제29조, 시행령 제30조, 개인정보의 안전성 확보조치 기준 제6조)

개인정보를 정보통신망을 통하여 송신 또는 보조저장매체를 통해 전달하는 경우에는 암호화 등을 하여야 하고, DB 또는 파일 등으로 저장하는 경우에는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장·관리하여야 한다.(법 제29조, 시행령 제30조, 개인정보의 안전성 확보조치 기준 제7조)

개인정보처리시스템별 안전성확보에 필요한 필수 요건 사항을 점검한다.

개인정보처리시스템 자율 점검표

점검 항목	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
1	내부 관리계획의 이행 실태를 연 1회 이상으로 점검·관리하는지 여부				
2	① 업무 위탁 계약문서에 필수 반영사항(7개)이 포함되었는지 여부 ※ 법 제26조 제1항 및 시행령 제28조 제1항 참조 ② 수탁자가 제3자에게 다시 위탁하는 경우 위탁자의 동의 여부				
3	내부 관리계획 수립·시행여부 [필수 18개 항목] ※ 개인정보의 안전성 확보조치 기준 제4조 제1항 참조				
4	개인정보처리방침의 공개 및 필수 사항 포함 여부 ※ 법 제30조 제1항 및 시행령 제31조 제1항 참조				
5	개인정보파일을 운용하는 경우 개인정보보호 종합지원 시스템(intra.privacy.go.kr)에 등록여부				
6	개인정보 제3자 제공 절차 수립 및 전파하고 개인정보 보호책임자 확인 하에 이행준수 여부				
7	개인정보 파기절차 수립 및 전파하고 개인정보 보호책임자 확인 하에 이행준수 여부				

점검 항목	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
8	개인정보 수집에 따른 정보주체의 동의 여부				
9	개인정보 수집·이용 동의를 받는 경우, 필수사항(4개) 고지 및 내용의 적정성 여부				
10	만 14세 미만 아동의 개인정보 처리 시 법정대리인(부모 등)의 동의 및 확인 여부				
11	제3자에게 개인정보 제공시 법률 근거 여부, 정보주체의 동의 여부 및 동의를 받을 때 필수 사항(5개) 고지 및 내용의 적정성 여부				
12	민감정보, 고유식별정보 수집에 따른 법령 근거 유무 또는 별도의 동의를 받고 있는지 여부				
13	법령에 근거하지 않고 주민등록번호를 수집 및 처리하고 있는지 여부				
14	개인정보(개인정보 파일) 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 영구 삭제하고 있는지 여부				
15	접근권한 관리 정책서 보유 여부[필수 사항 반영 여부] ① 접근권한 정의 및 업무분장, 책임 및 역할 ② 권한 부여 기준(업무담당자별(1인 1계정) 차등 부여, 말소 기준 등) ③ 권한 부여·변경·말소 절차 및 방법				
16	접근권한의 부여·변경·말소 내역을 기록 및 관리하고, 최소 3년간 보관하는지 여부				
17	안전한 비밀번호 작성규칙을 수립 및 적용하는지 여부				
18	일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등의 기술적 조치 여부				
19	개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하거나 접속한 IP주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응 여부 ※ 관리자페이지 외부 노출 여부				

점검 항목	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
20	외부에서 개인정보처리시스템에 접속하려는 경우, 안전한 접속수단* 또는 안전한 인증수단을 적용하는지 여부 * VPN 또는 전용선				
21	물리적 보관 장소의 안전조치 여부				
22	고유식별정보를 처리하는 경우 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점 점검여부				
23	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하는지 여부				
24	고유식별정보, 비밀번호, 생체인식정보, 신용카드번호, 계좌번호를 정보통신망을 통하여 송신하거나, 보조저장매체 등을 통하여 전달하거나, 저장하는 경우 안전한 암호알고리즘으로 암호화 적용 여부				
25	비밀번호 암호화 저장 시 일방향 암호화(해쉬함수) 알고리즘 적용 여부				
26	고유식별정보를 인터넷과 내부망의 중간지점(DMZ) 및 내부망에 저장하는 경우 암호화 조치 적용 여부				
27	안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차의 수립·시행 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관만 해당				
28	개인정보취급자의 접속기록을 최소 1년 이상 보관 및 관리하고, 도난 및 분실되지 않도록 안전하게 보관 및 관리하는지 여부 ※ 5만명 이상 또는 고유식별정보나 민감정보의 경우, 2년 이상 보관				
29	개인정보취급자의 접속이력 기록 시 필수 항목(5개)을 기록하고 있는지 여부 ※ 계정/접속일시/접속지정보/수행업무/처리한 정보주체의 정보				
30	월 1회 이상 접속기록 점검 여부(다운로드가 있을 경우 사유 확인 여부)				

점검 항목	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
31	보안 프로그램(백신)을 정당한 사유가 없는 한 자동 업데이트 또는 1일 1회 이상 업데이트하여 최신의 상태로 유지하고 있는지 여부				
32	개인정보 침해사고 대응 절차서[필수 4가지 사항 반영 여부] 수립 및 전파여부 ① 개인정보 침해 유형별 정의(유출, 노출 등) ② 업무 절차(침해사고 인지, 경위 조사, 확산 방지 등) ③ 업무 분장(개인정보 보호책임자, 개인정보 보호담당자, 개인정보취급자 등) ④ 신고 및 피해구제 방법(유출 신고, 통지 등)				
33	재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차 마련·점검 및 전파 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관만 해당 ① 개인정보처리시스템 구성 요소(개인정보 보유량, 종류·중요도, 시스템 연계 장비·설비 등) ② 재해·재난 등에 따른 파급효과(개인정보 유출, 손실, 훼손 등) 및 초기대응 방안 ③ 개인정보처리시스템 백업 및 복구 우선순위, 목표 시점·시간 ④ 개인정보처리시스템 백업 및 복구 방안(복구센터 마련, 백업계약 체결, 비상가동 등) ⑤ 업무분장, 책임 및 역할 ⑥ 실제 발생 가능한 사고에 대한 정기적 점검, 사후처리 및 지속관리 등				
34	재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획 마련 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관만 해당				

3. 업무용PC, 모바일 기기 등에 대한 관리 점검

개인정보취급자들이 사용하는 업무용 컴퓨터 등에 불필요한 개인정보가 보관되거나, 암호화되지 않은 상태로 보관되는 등 저장된 개인정보가 유·노출되지 않도록 정기적으로 점검 프로그램을 수행하거나 인터넷 홈페이지, P2P, 공유폴더, 무선랜 등 비인가 접근 경로를 차단하여야 한다. 또한, 개인정보를 기재한 문서에 대한 보안 관리를 취하여야 한다.(법 제29조, 시행령 제30조, 개인정보의 안전성 확보조치 기준 제6조)

업무용PC · 모바일 기기 개인정보 관리 점검표

점검 항목	세부 점검 내용	예	아니오	해당 없음
1	공유폴더 내 개인정보가 저장되어 업무용PC 등을 통해 공유되지 않도록 하는가?			
2	업무용PC 및 모바일 기기 사용 시 개인정보를 암호화하고 저장하는가?			
3	업무용PC에서 보조저장매체 이용 시 개인정보 유·노출 방지 조치가 되어 있는가?			
4	업무용PC에서 상용 웹메일, P2P, 웹하드, 메신저, SNS서비스 등 이용 시 개인정보 유·노출 방지 조치가 되어 있는가?			
5	업무용PC 및 모바일 기기 사용 시 비밀번호 설정 등의 보호조치 및 관리가 되고 있는가?			
6	업무용PC 내 PMS(개인정보관리솔루션) 등의 개인정보 관리를 위한 보안프로그램이 설치되어 운영 및 점검·관리되고 있는가?			