2022년 하반기 개인정보 처리 유의사항 안내

< 정보보호팀, '22. 9. 5. >

❖ **학생, 학부모 등의 개인정보 수집·이용이 집중되는 시기에 불필요한 개인정보 수집 방지와 개인정보 유출 예방을 위해 준수해야 할 유의사항 안내**

1 이메일, 메신저 등을 이용한 개인정보 처리

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

○ 상호 간에 실시간 정보공유가 가능한 **기관 메신저** 등을 이용하여 업무정보를 주고받는 경우, **개인정보 탑재 지양**

○ **공문**(붙임파일 포함)에 **개인정보**가 **포함**된 경우, **보안 결재, 열람범위 지정, 열람제한 등**의 기능을 활용하여 개인정보 유·노출 주의

⦿ 개인정보 유출사례

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

☞ SNS **단체 대화방, 메신저** 등을 통해 직원이 다수 학생에게 공지사항을 안내하며 개인정보 포함된 자료를 공유하는 사례

☞ **주소 변경 등을 이유로 다수 학생의 개인정보를 공유**하는 사례

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

2 개인정보처리시스템, 홈페이지 등에서의 개인정보 처리

○ 개인정보처리시스템에서 **초기 패스워드가 시스템에 의해 할당**되는 경우, 개인정보유출 예방을 위해 패스워드 변경 등 **관리 철저**

○ **홈페이지 파일**(한글, PDF 등) **탑재**, 강당·벽면·교내 **게시판**에 **자료 공지 시 개인정보 포함여부** 반드시 **확인**

- 홈페이지에 첨부파일을 게시하는 경우, **엑셀문서 지양**(PDF변환 게시 권고)

※ 부득이한 경우 비밀번호 설정 및 숨기기 처리된 시트·행·열 사전 확인 후 탑재

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

⊙ 개인정보 유출사례
☞ 반 편성 정보를 알리는 과정에서 성적 등 다수에게 공개되지 않아도 되는 불필요한 **개인정보가 포함된 자료**를 **게시**한 사례
☞ 개인정보가 없음을 **육안으로 확인**했음에도 **엑셀의 숨기기 기능에 의해** 드러나지 않던 **개인정보가 발견되어 유출**되는 사례

3 개인정보 수집 · 이용

○ 정보주체의 동의, 법령상 의무 준수, 공공기관의 소관 업무 수행 등을 위해 개인정보 수집·이용 가능(법 제15조)

- **(필수 고지사항)** 개인정보의 **①수집 목적, ②수집 항목, ③이용 기간, ④동의 거부권과 그에 따른 불이익 내용** 고지 후 동의
- **(별도 동의) 민감정보, 고유식별정보**(주민등록번호 제외) **등의 수집·이용 동의**는 다른 개인정보의 동의와 구분하여 **별도 동의** 필요
- **(주민등록번호 처리 제한)** 주민등록번호는 정보주체의 동의가 있어도 **법률, 시행령에 근거가 없으면 수집 불가**
- **(만14세 미만 아동의 개인정보 처리) 법정대리인의 동의 필수**

○ 개인정보는 처리 목적에 따라 **필요한 최소한의 정보만 수집**하고, 목적에 맞는 용도로 활용(법 제3조, 제16조)

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

⊙ 법 위반사례
☞ **(최소수집 위반)** 학사업무와 무관한 학부모의 직업, 학력, 생년월일 등 개인정보를 **과도하게 수집**하는 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

4 개인정보 제3자 제공 · 위탁

○ **(제3자 제공)** 기 수집한 개인정보를 수집한 **목적內 또는 목적外로 제3자에게 이용·제공**할 경우, **개인정보 보호법 준수**

- (**목적內**) 정보주체 동의*, 다른 법률에 규정, 공공기관 소관 업무 수행 등의 경우, **수집목적의 범위 내에서** 제3자 제공 가능(법 제17조)

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

- (**목적外**) 정보주체 동의, 다른 법률에 규정(국정감사 등), 범죄 수사, 법원 재판 등의 경우, **수집목적 외의 용도로** 제3자 제공 가능(법 제18조)

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

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

※ 수학여행, 졸업앨범 제작 등을 위해 업체 위탁 시 **수탁자 관리·감독 철저**

⊙ 법 위반사례

☞ **학사업무**를 **목적**으로 수집한 학생의 개인정보를 **홍보·마케팅 등** 수집 목적 범위를 초과하여 이용하거나 **제3자에게 제공**한 사례

☞ **민원업무로 알게 된** 민원인의 성명, 연락처 등의 **개인정보**를 정당한 이유 없이 **피민원기관에 제공**한 사례

☞ 민원인이 선생님의 핸드폰번호를 요구하여, **해당 선생님의 동의 없이 핸드폰번호**를 **제공**한 사례

5 개인정보 파기

○ 개인정보의 **보유기간 경과, 처리목적을 달성**한 경우, 별도의 보관 기간이 규정되어 있지 않다면, **지체 없이(5일 이내) 파기**(법 제21조)

※ CCTV 영상은 특별히 보관기간을 설정하고 있지 않다면 30일 동안 보관 후 파기

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

⊙ 파기 참고사례

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

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

☞ 부득이하게 개인정보를 포함한 파일을 **(업무용)PC에 저장**할 경우 **암호화하여 저장**하고 **목적 달성 시 즉시 파기** 조치

6 영상정보처리기기 운영

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

<영상정보처리기기 설치·운영 허용>

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

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

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

○ **(비공개된 장소)** 비공개 장소에 업무를 목적으로 영상정보처리기기를 설치하는 경우에는 **개인정보보호법 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)** 영상정보처리기기 운영자는 다음의 **필수사항**이 모두 **포함된 안내판 설치** 필요

안내판 필수사항

① 설치목적 및 장소
② 촬영범위 및 시간
③ 관리책임자 성명 및 연락처
④ 영상정보처리기기 설치·운영 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

○ (열람 등 요구 절차) “10일 이내” 처리 필요

열람대상		열람 등의 정구		본인 또는 정당한 대리인 여부 확인		열람 여부 결정		열람 조치		열람 기록·관리
1, 정보주체 2. 명백히 정보주체의 급박한 생명,신체, 재산의 이익을 위해 필요한 경우	⇒	정보주체의 개인영상정보 열람 또는 존재확인 요청	⇒		⇒	※ (열람 거부 사유) 1. 법률에 따라 제한된 경우 2. 타인의 생명·신체를 해하거나 재산 등을 침해할 우려가 있는 경우 3. 보관기간이 경과하여 파기한 경우 4. 범죄수사 등 5. 기타 정보주체의 열람 등 요구를 거부할 정당한 사유가 있는 경우	⇒	비식별조치가 가능한 경우	정보주체 외 모자이크 처리	⇒	개인영상정보 관리대장 기록 및 관리
								비식별조치가 어려운 경우	타 정보주체의 제3자 제공 동의 징구	

⊙ 법 위반사례

☞ 00고등학교 **화장실**에 학생 흡연 및 학교 폭력 방지를 위한 목적으로 CCTV를 **설치**하여 과태료 처분 받은 사례

7 개인정보처리자의 주요업무

○ 개인정보 내부관리계획에 따라 **안전조치의무(법 제29조) 이행사항**을 **주기적**으로 **철저하게 관리**(개인정보보호위원회 현장점검 시 주요점검 항목) **[붙임] 참조**

- 접속기록(매월 점검, 특히 다운로드 사유 확인), 접근권한 부여 및 관리 등
- 개인정보처리 위탁계약 시 수탁자의 업무 관리·감독 등
- 안전한 접속수단 및 인증수단 적용, 아이들 타임아웃(Idle Timeout)* 설정, 웹 취약점 점검 및 보완 조치 등 접근통제 강화

  * 최대 접속시간 제한 설정

- 전산실·자료보관실의 출입통제 철저 및 서류·보조저장매체 등을 안전한 장소에 보관

※ 공무원이 영리를 목적으로 개인정보를 유출한 사건과 유사사례가 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 접근 통제 강화 필요

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

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

- 개인정보 담당자(연1회 이상 교육 필수), 취급자는 기본적인 **개인정보보호 교육 실시 후 업무 투입**(법 제28조)

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

- **원격수업**을 **실시**하는 경우 **학생, 교사** 등을 **대상**으로 개인정보의 유출 예방 및 정보주체의 권리 보호를 위한 **사전 유의사항 안내**

※ 원격수업 중 불법적인 녹음, 녹화 등으로 인한 교육활동 침해 예방(교원지위법 제15조)

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

○ **1명 이상의 개인정보 유출 시** 상급기관 경유하여 **교육부 개인정보보호 포털**(https://privacy.moe.go.kr)에 **보고**하고 신속한 조치*

* 교육부 개인정보 유출사고 대응 매뉴얼, 개인정보보호 업무사례집 참조

※ **1천명 이상**의 **유출** 시, **교육부와 개인정보보호위원회**에 **신고**

8 참고사항

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

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

○ '개인정보 보호법', '교육부 개인정보 보호지침' 등 **관계법령 및 행정규칙**은 **국가법령정보센터(law.go.kr)**에서 확인 가능

[붙임]

교육기관

개인정보 안전성 확보조치(법 제29조) 체크리스트

《 개인정보 관리 현황 》

정보주체 수	000,000건 (000,000명)
개인정보파일 수	00개
개인정보처리시스템 수	00식
고유식별정보 보유 현황	□주민등록번호 □여권번호 □외국인등록번호 □운전면허 전체 정보주체 수 000건 (000명)
비 고	

□ 개인정보처리시스템 현황

개인정보 처리시스템명	개인정보 파일명(DB명)	정보주체 수 (명)	처리하는 개인정보 항목 ※ 필수/선택 구분	민감정보 및 고유식별정보 처리 여부	비고
TM시스템	*TM 고객정보*	*5,000,999건 (100,999명)*	*(필수) 고객명,연락처 등 (선택) 주소, 건강*	*· 민감정보(건강)*	
대표홈페이지 시스템	*홈페이지 회원정보*	*건수 확인불가 (100,999명)*	*(필수) 이름, 성명, 아이디, 비밀번호 CI (선택) 자택주소*	*· 처리하지 않음*	
예약관리시스템	*비회원 구매내역*	*1.000,999건 (10,999명)*	*(필수) 이름, 성명, 카드번호, 주소, 이메일주소, 연락처*	*· 고유식별정보(주민등록번호)*	
예약정보	*예약정보*	*건수 확인불가 5,999,999명*	*(필수) 영문이름, 한글이름, 연락처, 여권번호, 주민번호 (선택) 건강*	*· 고유식별정보(여권정보,주민등록번호)*	

개인정보처리시스템 자율 점검

◦ 개인정보처리시스템에 불법적인 접근 및 침해사고 방지 등을 위해 접근 제한 및 접근 통제를 위한 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)

개인정보처리시스템 자율 점검표

☐ 개인정보처리시스템명 (서비스명) ※ 개인정보처리시스템(서비스)별 점검 필요

점검 항목	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
1	내부 관리계획 수립·시행 여부 [필수 15개 항목]				
2	내부 관리계획의 이행 실태를 연 1회 이상으로 점검·관리하는지 여부				
3	접근권한 관리 정책서 보유 여부[필수사항 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				
4	접근권한의 부여·변경·말소 내역을 기록 및 관리하고, 최소 3년간 보관하는지 여부				
5	안전한 비밀번호 작성규칙을 수립 및 적용하는지 여부				
6	계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등의 기술적 조치 여부				
7	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)
8	외부에서 개인정보처리시스템에 접속하려는 경우, 안전한 접속수단* 또는 안전한 인증수단을 적용하는지 여부 * VPN 또는 전용선				
9	고유식별정보를 처리하는 경우 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점 점검 여부				
10	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하는지 여부				
11	고유식별정보, 비밀번호, 생체인식정보를 정보통신망을 통하여 송신하거나, 보조저장매체 등을 통하여 전달하거나, 저장하는 경우 안전한 암호 알고리즘으로 암호화하는지 여부				
12	비밀번호 저장 시 일방향 암호화(해쉬함수) 적용 여부				
13	고유식별정보를 인터넷과 내부망의 중간지점(DMZ) 및 내부망에 저장하는 경우 암호화 조치 적용 여부				
14	안전한 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차의 수립·시행 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관(강화유형)만 해당				
15	개인정보취급자의 접속기록을 최소 1년 이상 보관·관리하고, 위·변조 및 도난, 분실되지 않도록 안전하게 보관하는지 여부 ※ 5만명 이상 또는 고유식별정보나 민감정보의 경우, 2년 이상 보관				
16	개인정보취급자의 접속기록에 필수 항목(5개)을 포함하여 기록·관리하고 있는지 여부 ※ 계정/접속일시/접속지 정보/수행업무/처리한 정보주체의 정보				
17	월 1회 이상 접속기록 점검 여부(다운로드가 있을 경우 사유 확인 여부)				
18	보안 프로그램(백신)을 자동 업데이트 또는 1일 1회 이상 업데이트하여 최신 상태로 유지하고, 악성 프로그램 등에 대해 즉시 대응 조치하고 있는지 여부				

점검 항목	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
19	관리용 단말기에 대한 안전조치 여부				
20	물리적 보관 장소의 안전조치 여부				
21	개인정보 침해사고 대응 절차서[필수 4가지 사항 반영 여부] 수립 및 전파 여부 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)				
22	재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차 마련·점검 및 전파 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관(강화유형)만 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, 목표시점·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				
23	재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획 마련 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관(강화유형)만 해당				
24	개인정보 파기 시 복구가 불가능한 방법*으로 파기하고 있는지 여부 * 완전파괴(소각·파쇄 등), 전용 소자장비, 데이터 초기화 등				

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 수행해야 한다. 또한, 홈페이지, P2P, 공유폴더, 무선랜 등 비인가 접근 경로를 차단하고 개인정보를 기재한 문서에 대한 보안 관리를 취하여야 한다.(법 제29조, 시행령 제30조, 고시 제6조)

업무용PC 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?			