

11 개인정보의 유출통지 및 신고

관련근거

- ▶ 개인정보 보호법 제34조(개인정보의 유출 통지 등)
- ▶ 개인정보 보호법 시행령 제39조(개인정보 유출 신고의 범위 및 기관), 제40조(개인정보 유출 통지의 방법 및 절차)
- ▶ 교육부 개인정보 보호지침 제50조 ~ 제53조

업무시기

- ▶ 사안 발생 시

주요내용

□ 개인정보 유출의 개념

- 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인 정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것으로서, 다음 중 어느 하나에 해당하는 경우를 말함

〈개인정보 유출의 종류(교육부 개인정보 보호지침 제50조)〉

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 그 밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우
4. 그 밖에 권한이 없는 자에게 개인정보가 전달된 경우

□ 개인정보 유출사고 대응 절차

절차	주요내용
사고인지 및 긴급조치	• 개인정보 유출사고 신고접수 및 사고인지 • 유출사고 대응반 소집 및 유관기관 협조체계 확인 • 피해 최소화를 위한 긴급조치 수행
↓	
정보주체 유출통지	• 정보주체에게 개인정보 유출사실 통지(5일 이내)
↓	
개인정보 유출신고	• 1건이라도 개인정보 유출시 반드시 신고 - 유출내용 및 조치결과를 5일 이내에 상급기관 보고 및 교육부 신고* * 교육부 개인정보 유출 신고 센터(privacy.moe.go.kr)에 유출 기관이 직접 신고 • 1천명 이상의 개인정보 유출시 교육부 및 개인정보보호위원회(한국인터넷진흥원, privacy.go.kr)에 추가 유출 신고
↓	
민원대응 및 피해구제 절차	• 개인정보 유출사고 규모 및 성격에 따라 민원대응반 구성 • 2차 피해 방지를 위한 민원 대응 및 불안 해소 조치 • 개인정보 유출에 대한 피해구제 절차 안내
↓	
보안기능 강화 및 재발방지	• 사고 원인 분석 및 보안 강화·기능 개선 • 기관장에 개인정보 유출사고 결과보고서 작성 및 보고 • 개인정보 유출사고 사례 전파 교육 및 개선 대책 시행

※ 개인정보 보호담당자는 취급하는 개인정보에 대하여 유출이 발생한 것으로 인지한 경우 또는 민원인의 신고를 받은 경우 유출사실 여부를 확인하고 유출사고 접수 후 지체 없이 개인정보 보호책임자 및 지도·감독기관의 개인정보 보호책임자에게 유출사고를 보고하여야 함

□ 정보주체 유출통지 방법

통지대상	▶ 정보주체
통지방법	▶ 서면, 전자우편, FAX전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법 ▶ 위의 통지방법과 동시에 홈페이지 공개 - 1천명 이상의 개인정보가 유출된 경우에는 서면 동의 방법과 함께 인터넷 홈페이지에 7일 이상 통지내용을 게재
통지내용	①유출된 개인정보의 항목 ②유출 시점과 그 경위 ③피해 최소화를 위한 정보주체의 조치방법 ④기관의 대응조치 및 피해구제 절차 ⑤피해 신고 접수 담당부서 및 연락처
통지시기	▶ 유출사실을 알게 되었을 때에는 지체없이(5일 이내)
통지연기	▶ 개인정보 유출확산방지를 위한 조치가 필요한 경우 연기 가능 - 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속권한 삭제·변경 또는 폐쇄 조치 - 네트워크, 방화벽 등 대·내외 시스템 보안점검 및 취약점 보완조치 - 향후 수사에 필요한 외부의 접속기록 등 보존 조치 - 정보주체에게 유출 관련 사실을 통지하기 위한 유출확인 웹페이지 제작 등의 통지방법 마련 조치 - 기타 개인정보의 유출확산 방지를 위한 필요한 기술적·관리적 조치 ▶ 개인정보처리자는 위 각 항목의 조치를 취한 이후, 정보주체에게 다음 각 항목의 사실만 일차적으로 알리고 추후 확인되는 즉시 알릴 수 있음 - 정보주체에게 유출이 발생한 사실 - ‘통지내용’ 중 확인된 사항

□ 유출 신고방법

신고대상	▶ 1명이라도 개인정보 유출 시, *상급기관 및 교육부에 신고 *상급기관: (유·초·중) ⇨ 관할교육지원청, (직속,고) ⇨ 본청 디지털·혁신미래교육과 ▶ 단, 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우 개인정보보호위원회 또는 한국인터넷진흥원에 추가 신고
신고시기	지체 없이(5일 이내)
신고방법	▶ 공문(상위기관), 인터넷 사이트를 통해 유출사고 신고 및 신고서 제출 - 교육부: privacy.moe.go.kr , 개인정보보호포털: privacy.go.kr
신고내용	▶ 기관명, 통지여부, 유출된 개인정보 항목·규모, 유출 시점·경위, 유출피해 최소화 대책·조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서·담당자 연락처 등 ※ 정보주체에 대한 유출 통지 결과 및 피해 최소화를 위한 조치 결과가 포함되도록 해야 함
신고양식	▶ 개인정보 유출신고서

유의사항

- ☞ 개인정보처리자는 유출사고 최초 발생 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실 유무 입증책임을 짐

벌칙 과태료

- ▶ 정보주체에게 유출통지 아니한 자(법 제34조제1항 위반)
: 3천만원 이하의 과태료 [법 제75조제2항제8호]
- ▶ 개인정보 유출 조치결과를 신고 하지 아니한 자(법 제34조제3항 위반)
: 3천만원 이하의 과태료 [법 제75조제2항제9호]

참고

- ▶ 표준 개인정보 유출 통지 문안(예시)
- ▶ 개인정보 유출 신고 보고 기안문(예시)
- ▶ 개인정보 유출신고(보고)서(양식)
- ▶ 개인정보 유출신고서 작성 사례

- ☐ 부가설명란에 필수사항은 (< >), 참고사항은 ()로 표기하였음
- ☐ 필수사항은 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인되면 반드시 추가 통지
- ☐ 아래 예시를 참고하여 유출 상황에 적합하게 내용을 변경하여 활용

표준 통지문안 예시	부가 설명
개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.	< 제목 > - ‘유출 통지’문구 포함
귀하의 개인정보 보호를 위해 최우선으로 노력하여 왔으나, 불의의 사고로 귀하의 소중한 개인정보가 유출되었음을 알려 드리며, 이에 대하여 진심으로 사과를 드립니다.	(사과문) - 유출 통지 사실 알림 - 사과문을 먼저 표현
귀하의 개인정보는 20○○년 ○월 ○일 000시스템 장애처리를 위한 데이터 분석 과정에서 유지보수업체로 전달되었고, 유지보수 업체는 자체 서버에 저장·보관하다가 안전한 조치를 다하지 못해 20○○년 ○월경 해커에 의한 해킹으로 유출되었습니다. 유출된 정확한 일시는 대구지방경찰청에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.	<유출된 시점과 경위> - 유출된 시점과 경위를 누구나 이해할 수 있게 상세하게 설명 - ‘귀하’, ‘고객님’ 등으로 유출된 정보주체 명시 ※ 부적합한 표현 : 일부 고객, 회원정보의 일부 등 - 추가 확인된 사항은 반드시 추가로 통지
유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 연락처로 총 6개입니다.	<유출된 항목> - 유출된 항목을 누락 없이 모두 나열 ※ ‘등’으로 생략하거나, ‘회사 전화번호’ 및 ‘집 전화번호’를 합쳐서 ‘전화번호’로 표시 안됨
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	<개인정보처리자의 대응조치> - 접속경로 차단 등 예시된 항목 외에도 망 분리, 방화벽, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등의 조치한 내용 설명



○○○학교

다양성이 꽃피는
공존의 혁신미래교육

수신자 서울특별시○○교육지원청교육장(행정지원과장)

수신자

(경유)

제목 ○○○학교 개인정보 유출 신고(보고)

1. 관련: 교육부 개인정보 보호지침 제53조(개인정보 유출신고)
2. 개인정보 유출사고가 발생하여 유출내용 및 조치결과를 붙임과 같이 보고합니다.

붙임 개인정보 유출신고(보고)서 1부. 끝.

★

교장

협조자

시행 ○○학교-0000 (0000. 00. 00.) 접수

()

우 00000 서울특별시 ○○○○○○

/ http://www.

전화 02-000-0000

/전송 02-000-0000

/ ○○○@○○○

/ 비공개(7)

■ 교육부 개인정보 보호지침 [별지 제5호 서식]

개인정보 유출신고(보고)서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수기관	기관명	담당자명	연락처

개인정보 유출 신고서(작성 예시)

기관명	00고등학교				
정보주체에의 통지 여부	■ 통지일자: 2022. 3. 22. (화) ■ 통지방법: 이메일 및 유선 전화 ■ 통지대상: 정보주체 1,100명(학생 600명, 학부모 200명, 교직원 300명)				
유출된 개인정보의 항목 및 규모	■ 유출규모: 1,150명(중복제거 후 1,100명) - 교육부 신고여부(○), 개인정보위 신고여부(○), 홈페이지 공개여부(○) ■ 유출항목: 이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일				
유출된 시점과 그 경위	■ 사고발생 인지경로 - 2022.3.21 10:00 월별 개인정보처리시스템 접속로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인 - 2022.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견 - 2022.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인 ■ 유출 시점 및 경위 - 2022.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드 - 2022.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송				
유출피해 최소화 대책·조치 및 결과	■ 정보주체가 할 수 있는 피해최소화 방법 ① 2차 피해 방지를 위하여 개인정보 유출 여부 조회(학교 홈페이지 등) ② 유출사고 발생 후 홈페이지 로그인시 개인정보 유출에 따른 비밀번호 변경 ■ 사고발생 후 조치사항 ① 기관 개인정보 유출사고 대응 매뉴얼에 따라 침해사고 대응반 구축 ② 개인정보 침해 접수 창구 및 민원 대응 창구 구축 ③ 유출 항목 및 발생 상황 인지 후 유출 통지문 작성 및 관련 내용 통지, 교육부 개인정보 유출 신고 ④ 유출 원인에 따른 개인정보처리시스템에 대한 접근권한 관리체계 강화 ⑤ 재발방지 대책을 위한 보안강화 계획(안) 수립				
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	① 2차 피해 접수를 위한 피해 접수 담당 창구 운영(02-124-2345, abcd@efgf.co.kr) ② 개인정보 유출 관련 개인정보 분쟁조정 신청 창구 안내(1833-6972)				
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자	김영희	총무과	교장	02-123-1234
	개인정보 취급자	홍길동	총무과	담당자	02-123-1234

유출신고접수기관	기관명	담당자명	연락처
	서울특별시교육청	김철수	02-123-5678