GYEONGSANG NATIONAL UNIVERSITY

FLY WITH GNU

경상국립대학교 Gyeongsang National University

「개인정보 유출사고 대응 매뉴얼」

2024. 8. 5.

경상국립대학교

[총 무 과]

[제·개정 이력]

순번	구 분	시행 일자	제정 · 개정 주요내용	작성자	승인자
1	제정	2014.06.07.	- 내부 개인정보 관리 안전성 확보를 위한 제정		
2	일부개정	2016.05.04.	1. 개인정보 보호법, 동법 시행령, 교육부 개인정보 보호지침에 따른 의무사항 반영 2. 개인정보 처리의 위탁 등 조문 신설 3. 개인정보 유출 등의 신고 조문 신설 등		
3	전부개정	2019.02.27.	1. 개인정보의 안전성 확보조치 기준에서 유형별로 정하는 사항 반영 2. 유형3(강화) 기관으로서 개인정보 내부관리계획 구성 항목의 충실한 반영		
4	일부개정	2022.05.18.	1.「개인정보 보호법」,「개인정보의 안전성 확보조치 기준」 개정 내용을 반영하여 일부 변경		
5	전부개정	2024.08.05.	1. 개인정보 유출등 용어 변경 및 개념 재정의 2. 개인정보 유출등의 통지 시점, 신고 대상, 규모 등 변경 3. 유출등 사고 대응에 대한 단계별 업무 프로세스 명확화		

목 차

❍ 본 매뉴얼은「개인정보 보호법」의 적용을 받는 개인정보처리자를 대상으로 합니다.

적용대상

업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통해 개인정보를 처리하는 대학의 모든 개인정보처리자

❍ 본 매뉴얼은 「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2024-1호, 2024.1.4.) 제29조(개인정보 유출등 사고 대응 매뉴얼 등)에 따라,

- 개인정보 유출등 사고와 관련하여 신속한 대응과 그 피해를 최소화하기 위한 최소한의 사항을 안내하고 있습니다.

관계법령

표준 개인정보 보호지침

제29조(개인정보 유출등 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출등 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출등 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출등 대응 매뉴얼에는 유출등 통지·조회 절차, 영업점·인터넷회선 확충 등 고객민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출등에 따른 피해복구 조치 등을 수행 함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

개인정보 유출등 대응 절차(요약)

1. 개인정보 유출등 대응 체계 구축

개인정보 유출등 사고 대응팀	**개인정보 보호책임자**	개인정보 유출등 대응 총괄 지휘, 개인정보 유출등 사고 대응팀 구성·운영
	개인정보 보호담당자	정보주체에게 개인정보 유출 통지, 교육부 또는 개인정보위에 개인정보 유출 신고
	정보보호 담당자	교육부에 침해사고 신고, 사고 경위 분석, 시스템 복구 등 침해 대응
	담당·지원 부서	정부, 언론사, 이용자 민원 대응, 이용자 피해구제 분쟁조정 기구 안내

2. 피해 최소화 및 긴급 조치

유형	**대응 방안**
해킹	시스템 분리/차단 조치, 로그 등 증거자료 확보, 유출 원인분석, 정보주체 및 개인정보 취급자 비밀번호 변경 등
내부자	유출 경로 확인, 유출에 활용된 컴퓨터/USB/이메일/출력물 등 확보, 취급자의 접근권한 확인, 비정상 접근 경로 차단 등
이메일	발송 이메일 즉시 회수, 수신자에게 오발송 메일 삭제 요청, 대용량 메일서버 운영자에게 파일 삭제 요청, 파일 전송 시 암호화 등
노출	검색엔진 : 노출된 개인정보 삭제 요청, 로봇(크롤링 등) 배제 규칙 적용 등 시스템 오류 : 소스 코드, 서버 설정 등 원인 파악 및 수정 등

3. 개인정보 유출등 통지 및 신고

근거법률		**개인정보 보호법**	**교육부 개인정보 보호지침**
		제34조(개인정보 유출 등의 통지·신고)	**제13조(개인정보 유출등의 신고)**
유출 통지	**규모**	1명 이상	
	시점	72시간 이내(유출등이 되었음을 알게 되었을 때)	
	방법	홈페이지, 서면 등의 방법으로 개별 통지	
	항목	① 유출등이 된 개인정보의 항목, ② 유출등이 된 시점과 그 경위 ③ 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법, ④ 개인정보처리자의 대응조치 및 피해구제 절차, ⑤ 피해 신고·상담 부서 및 연락처 등	
유출 신고	**규모**	① 1천명 이상 ② 1명 이상 민감정보, 고유식별정보 유출 등 ③ 외부로부터의 불법적인 접근에 의한 개인정보 유출 등	1명 이상
	시점	72시간 이내(유출등이 되었음을 알게 되었을 때)	
	기관	개인정보보호위원회 또는 한국인터넷진흥원 (privacy.go.kr)	교육부 또는 한국교육학술정보원 (privacy.moe.go.kr)

4. 피해 구제 및 재발 방지

정보주체 피해구제	- 홈페이지 등을 통한 유출 여부 조회 기능 제공 - 유출로 인한 피해 신고, 접수, 상담, 문의 등 각종 민원 대응 방안 마련 - 유출 대응 현장 혼란 최소화 방안 강구 - 보이스피싱 등 2차 피해 방지를 위한 유의 사항 안내 - 피해 보상 계획 마련 및 관련 제도 안내 등
재발 방지 대책 마련	- 개인정보 유출 원인 등에 대한 개선 방안 마련 - 취급자 대상 개인정보보호 교육 실시 - 홈페이지 취약점 제거 등 개인정보 안전조치 강화 등

1 개요

1.1 목적

❍ ‘개인정보 유출등 사고 대응 매뉴얼’은 대학이 ‘개인정보 보호법’ 및 시행령, 관련 지침에 따라 개인정보 유출등 관련 사고에 대하여 신속하고 체계적인 대응을 목적으로 한다.

※ 관련근거 : 표준 개인정보 보호지침 제29조(개인정보 유출등 사고 대응 매뉴얼 등)

1.2 법적 근거

❍ 개인정보 보호법 및 시행령

❍ 표준 개인정보 보호지침, 개인정보의 안전성 확보 조치 기준

❍ 경상국립대학교 개인정보 보호지침

1.3 용어 정의

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 것을 말한다.

용 어	정 의
유출등 사고 대응팀	• 개인정보 유출등 사고 발생에 따른 사고의 분석, 처리지원, 사후 복구, 사후 예방조치 등을 주요 업무로 하는 개인정보보호 담당 부서를 말함
개인정보 보호책임자	• 개인정보 보호법 제31조에 근거하여 개인정보 처리 업무를 총괄하는 자 • 개인정보 보호담당자를 임명하여 유출등 사고 발생 시 본 절차에 따라 대응토록 함
개인정보 보호담당자	• 개인정보 보호책임자의 지정을 받아 개인정보 보호 업무를 수행하는 자
분야별 책임자	• 개인정보 보호책임자의 지휘·감독을 받아 각 업무부서의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말함
분야별 담당자	• 개인정보보호 분야별 책임자의 지정을 받아 개인정보 보호 업무를 수행하는 자
개인정보취급자	• 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말함

참고자료

대법원 2014. 5. 16. 선고 2011다24555, 24562판결

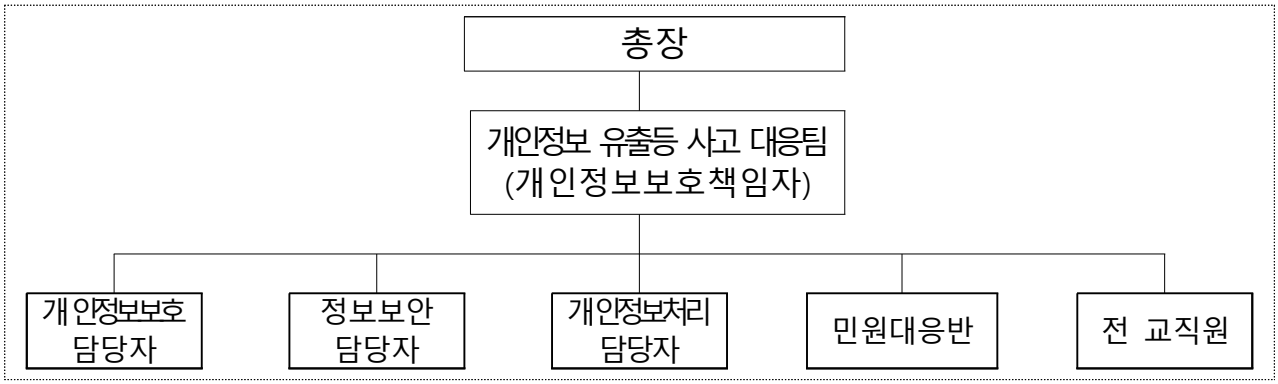
개인정보의 **누출**이란 개인정보가 해당 정보통신서비스 제공자의 **관리 · 통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 의미하는바,** 어느 개인정보가 정보통신서비스 제공자의 관리 · 통제하에 있고 그 개인정보가 **제3자에게 실제 열람되거나 접근되지 아니한 상태**라면, 정보통신서비스 제공자의 기술적 · 관리적 보호조치에 미흡한 점이 있어서 제3자가 인터넷상 특정 사이트를 통해 정보통신서비스 제공자가 **보관하고 있는 개인정보에 접근할 수 있는 상태에 놓여 있었다고 하더라도 그것만으로 바로 개인정보가 정보통신서비스 제공자의 관리 · 통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 되었다고 할 수는 없다.**

1.4 단계별 프로세스(업무 절차)

단계	상세 업무	비고
사고인지 및 긴급 조치	○ 개인정보 유출등 사고 인지 및 신고 접수 - 유출등 사고 발생이 의심되는 경우, 지체없이 개인정보 보호담당자에게 신고 ○ 개인정보보호 담당자는 사고 내용 등에 대해 개인정보 보호 책임자에게 보고 ○ 유출등 사고 대응반 소집 및 유관기관 협조체계 확인 ○ 피해 최소화를 위한 긴급 조치 수행 - 유출등이 된 개인정보 비공개 또는 삭제 조치 - 유출등 접속경로 차단, 취약점 점검·보완 등 긴급 조치, 재발 방지 조치 등	
↓		
정보주체 유출등 통지	○ 정보주체에게 개인정보 유출등 사실 통지(**72**시간 이내) - 유출등이 된 개인정보의 항목, 유출등이 된 시점과 그 경위, 피해구제 절차 등	세부내용 2.1 참고
↓		
개인정보 유출등 신고	○ 1명 이상의 개인정보 유출등 발생 시 교육부(privacy.moe.go.kr)에 유출 신고 ○ ①1천명 이상 유출등이 발생하거나, ②민감정보·고유식별정보 1건 이상 또는 ③외부로부터의 불법적인 접근에 의해 1건 이상 유출등 발생 시 교육부 및 개인정보보호위원회(한국인터넷진흥원, privacy.go.kr)에 유출 신고	세부내용 2.2 참고
↓		
사고분석	○ 유출등 사고 대응반의 조사 및 분석 - 사고 원인 분석, 유출등 규모 확인, 사고 원인에 대한 조치 등	
↓		
민원 대응	○ 민원 대응을 위한 별도의 온·오프라인 창구 개설·운영 - 피해자 구제 방안, 수사 진행 상황 등에 대한 답변 방향 결정 및 응대 - 2차 피해 방지를 위한 조치 방법 안내 등 고객 불안 해소 조치 및 피해구제 절차 안내	세부내용 2.4~2.6 참고
↓		
유출등 사고 결과 보고	○ 개인정보 유출등 사고 결과보고서 작성 및 보고	
↓		
개선 및 이행점검	○ 개인정보 유출등 사고 사례 전파 교육 및 개선 대책 시행 (재발 방지)	

1.5 유출등 대응 업무수행 체계

❍ 조직체계



❍ 업무분장

조직	담당 업무
총장	• 유출등 대응 관련 방향성 제시, 의사 결정, 총괄 지휘
개인정보보호 책임자	• 유출등 사고 대응 총괄 지휘 및 사고 대응팀 구성·운영
개인정보 유출등 사고 대응팀	• 유출등 사고 인지, 접수, 전파 • 유출등 사고 대응 절차 수립 • 정보주체에게 유출등 사실 통지
개인정보보호 담당자	• 유출등 사실 확인, 조사 및 원인분석 • 교육부 및 개인정보위에 유출등 신고
정보보안 담당자	• 외부요인에 의한 유출의 경우, 유관기관과 협조하여 사고 처리지원 • 사고 내용 세부조사 및 분석 • 시스템 복구 및 백업(유지보수/협력업체 포함)
개인정보처리 담당자	• 유출등 사실 확인, 조사 및 자료 제출 • 총무과 및 정보전산처에 유출등 신고 • 개인정보 유출 신고서 작성 및 정보주체에게 유출등 통지
민원대응반 (온라인, 오프라인)	• 개별 통지문 안내에 따른 후속 업무(민원 등) 진행 • 정부, 언론사, 이용자 민원 대응 • 상담센터, 소비자보호 방안 마련(필요시 유관부서와 협조)
전 교직원	• 개인정보 유출 확인 시 부서장 및 개인정보보호 부서에 신고 • 침해사고 발생 확인 시 부서장 또는 정보보호 부서에 신고 • 개인정보 유출 신속대응팀 요청에 따른 유출 대응 지원

❍ 비상연락망

- 개인정보 유출등 사고 대응팀

조직별	담당자	전화번호	이메일
개인정보보호 책임자	사무국장 직무대리	055-772-0065	
개인정보보호 담당자	총무과 개인정보 보호 담당자	055-772-3141	leeod@gnu.ac.kr
정보보안 담당자	정보전산처 개인정보 담당자	055-772-0613	hancy@gnu.ac.kr
개인정보처리 담당자	개인정보처리 담당자		
민원대응반	총무과 감사팀장	055-772-3140	jinlove4865@gnu.ac.kr

- 협력업체/유지보수업체

업체명	담당 시스템	담당자	전화번호	이메일
투썸데이터	오라클DB	강경수(이사)	010-4568-4957	gsgang@2sumdate.com
아이웍스	IBM서버	이시원(책임)	010-5606-2689	lswon@iworks.kr
우리아이티	네트워크	전경인(이사)	010-5537-5138	kineon@wooriit.kr
신아시스템	방화벽, 보안	신동석(과장)	010-2909-2444	sindseok@sinasystem.com
아이시큐	DDoS, 서버팜방화벽	도현석(프로)	010-2039-3943	po22yaa@isecu.co.kr
네오비트	개인정보접속기록 관리시스템	유시승(과장)	010-9138-7803	yss21@neobit.kr

2 개인정보 유출등 사고 대응 조치 및 피해구제 방법

2.1 유출등 통지·조회 절차

가이드

o 개인정보처리자는「개인정보 보호법」제34조제1항에 따른 통지 절차를 마련하고 이에 대한 내용을 기술
o 개인정보처리자는 개인정보 유출등 사고 규모에 따라 신고 관련 절차를 마련하고 이에 대한 내용을 기술
o 개인정보처리자는 정보주체가 홈페이지 등을 통해 자신의 개인정보가 유출등이 되었는지 확인할 수 있는 절차를 만들고 이에 대한 내용을 기술
o 개인정보 처리 업무 위탁 시, 1차적인 유출등 신고 및 통지 의무는 위탁자에게 있으므로, 유출등 사고 발생 시 수탁자와의 대응 절차를 마련하고 이에 대한 내용을 기술

❍ 개인정보 유출등 사고 대응팀은 유출등이 된 규모 및 관련 사항을 확인하여 유출등 통지 방법*에 따라 정보주체들에게 개인정보 유출등 통지

* 본 매뉴얼 내 [개인정보 유출등 대응 절차(요약) - 3. 개인정보 유출등 통지 및 신고] 참고

- 통지 항목 : ① 유출등이 된 개인정보의 항목, ② 유출등이 된 시점과 그 경위, ③ 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법, ④ 개인정보처리자의 대응조치 및 피해구제 절차, ⑤ 피해 신고·상담 부서 및 연락처 등

❍ 수탁사업자가 수탁 업무를 처리하는 과정에서 개인정보가 유출등이 된 경우 즉시 위탁자에게 보고하도록 표준 개인정보처리위탁 계약서에 명시하고, 수탁사업자로부터 보고 받은 시점에서 지체없이 유출통지

❍ 1명 이상 개인정보 유출등이 되었음을 알게 되었을 때에는 서면 등의 방법으로 72시간 이내에 유출등 통지 항목 5개를 정보주체에게 안내

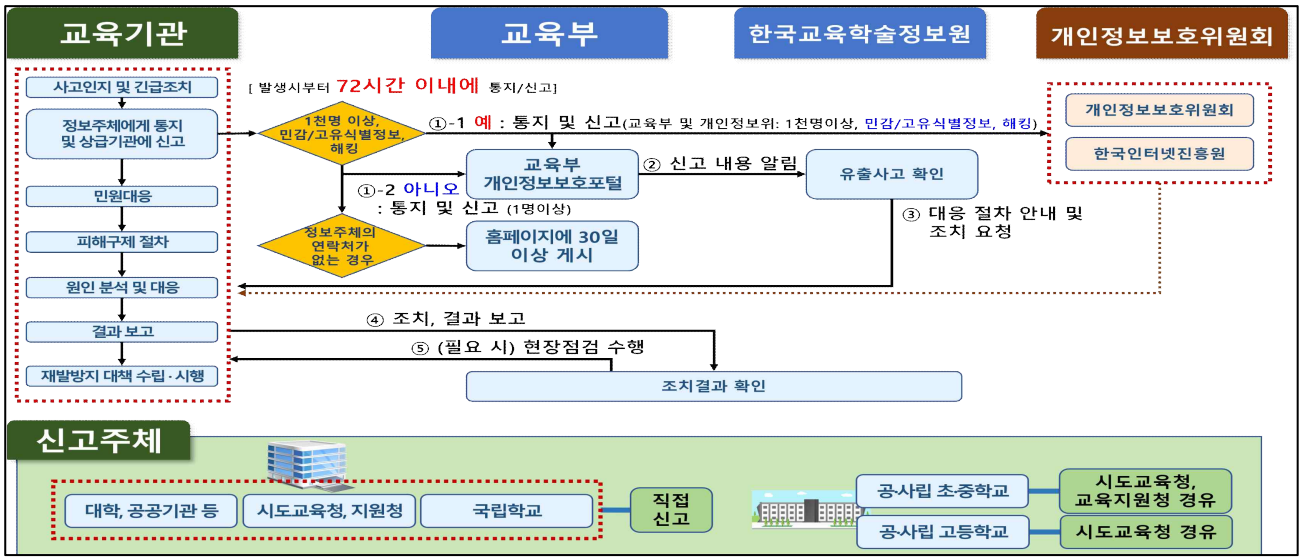
- 정보주체의 연락처를 알 수 없는 경우 인터넷 홈페이지에 통지 항목 5개를 30일 이상 게시하는 것으로 정보주체 유출등 통지 의무를 갈음할 수 있음

개인정보 유출등 통지문(예시)

통지문(예시)	작성 준수사항
개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.	
❶ 귀하의 개인정보는 ○○○○년 ○○월 ○○일 **해커에 의한 홈페이지 내 악성코드가 삽입**되어 **○○건이 유출**된 것으로 확인되었습니다. 유출된 정확한 일시는 에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.	❶ **개인정보 유출 등이 발생한 시점**과 확인한 유출 건수를 누구나 이해할 수 있게 상세하게 설명 ☞ 잘못된 사례: '회원 정보 일부' 등
❷ **유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(PW), 이메일, 휴대전화번호 총 5개 항목**입니다.	❷ **유출된 개인정보 항목**은 누락 없이 모두 나열하여야 함 ☞ 잘못된 사례: '등'으로 생략하거나, 회사 전화번호, 집 전화번호를 '전화번호'로 통칭
❸ 유출 사실을 인지한 후 **해당 악성코드는 즉시 삭제하였으며, 해커가 접속한 해당 IP와 우회 접속한 IP를 차단**하고, 추가적인 **홈페이지 취약점 점검과 보완 조치**를 하였습니다. 더불어 **침입방지 시스템을 추가 도입하여 24시간 모니터링**을 수행하고 있습니다.	❸ **개인정보처리자 등의 대응조치 내용** 접속경로 차단 등 예시된 항목 외에도 망 분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명
❹ 이번 사고로 인해 유출된 개인정보를 이용하여 웹사이트 명의도용, 보이스피싱, 파밍 등 **2차 피해의 우려**가 있으므로 혹시 모를 피해를 막기 위하여 **고객님의 비밀번호를 변경하여 주시기 바랍니다.**	❹ **이용자가 취할 수 있는 조치 방법** 유출된 개인정보, 경로 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내(예: 보이스피싱, 피싱 메일, 불법TM, 스팸문자 등)
❺ **비밀번호 변경하기**	❺ 이용자의 비밀번호 변경 페이지로 연결
❻ **개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 아래 피해 등 접수 담당부서로 연락해 주시기 바랍니다.** ▸ 피해 등 접수 담당부서: ○○○○(055-123-0000) ▸ 피해 등 접수 e-메일: ○○○○@oooo.co.kr 경상국립대학교	❻ **이용자가 상담 등을 접수할 수 있는 부서 및 연락처** 전담 처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내
❼ **개인정보 유출 여부 조회하기**	❼ **이용자가 자신의 개인정보 유출 여부를 조회**할 수 있도록 절차를 마련

2.2 유출등 신고 절차 및 방법

❍ 유출등 신고 절차



❍ 유출등 신고 방법

구분	내용
신고대상	▶ 개인정보가 1천명 이상 유출등이 됐거나, 민감정보·고유식별정보 및 외부로부터의 불법적인 접근에 의해 1건이라도 유출등이 된 경우는 **교육부 및 개인정보위**(또는 **한국인터넷진흥원**)에 신고 ▶ 1명 이상 유출등이 된 경우 상급 기관을 경유하여 **교육부**에 신고 ※ 대학은 **교육부**에 신고
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
신고방법	▶ 교육부(privacy.moe.go.kr) 및 개인정보보호위원회(privacy.go.kr) 홈페이지를 통해 유출등 신고서 제출 ※ 부득이한 경우 전자우편 등을 통해 개인정보 유출 신고서 제출 ▶ 시간적 여유가 없거나 특별한 사정이 있는 경우 상급기관과 교육부에 동시에 신고하며 유출등 신고서 제출
신고내용	▶ 기관명, 통지 여부, 유출등이 된 개인정보 항목·규모, 유출등 시점·경위, 유출등 피해 최소화 대책·조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차, 담당 부서·담당자 연락처 등 ※ 정보주체에 대한 유출등 통지 결과 및 피해 최소화를 위한 긴급 조치 내용이 포함되도록 해야 함
신고양식	▶ [붙임 1] 개인정보 유출등 신고서 (양식)

※ **조치결과**는 교육부 개인정보 보호지침 제14조(개인정보의 유출등 조사)에 따라 [붙임2] **개인정보 유출등 신고 조치확인서 작성 및 제출**(moeprivacy@keris.or.kr)

개인정보 유출등 신고서 작성 방법

유출 등 신고서 양식	작성 방법
❶ 유출등이 된 개인정보 항목	- 유출 등이 된 개인정보 항목을 모두 기재해야 하며, '등'과 같이 일부 생략하거나 휴대전화번호와 집 전화번호를 '전화번호'로 기재 하여서는 안됨 - 유출 등이 된 개인정보의 모든 항목을 적어야 하며, 유출 등 규모도 현시점에서 파악된 내용을 모두 작성
❷ 유출등이 된 시점과 그 경위	- 유출 등 시점, 인지 시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출 등 경위와 인지 경위를 포함
❸ 정보주체가 취할 수 있는 피해 최소화 조치	- 개인정보 유출 등으로 발생 가능한 스팸문자, 보이스피싱, 금융사기와 같은 2차적인 피해 방지를 위해 이용자가 할 수 있는 조치를 기재(예: 비밀번호 변경 등)
❹ 개인정보처리자 대응조치 및 피해 구제절차	- 유출 등 사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해구제를 위한 계획 및 절차를 기재 ex) 경찰에 신고, 일시적 홈페이지 로그인 차단(홈페이지 해킹일 경우) 등
❺ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처	- 실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자 연락처를 기재
❻ 기타	- 유출 등이 된 기관명, 사업자번호, 사업자 주소, 웹사이트 주소 등 기재

2.3 현장 혼잡 최소화 조치

가이드

o 유출 대응 현장에서의 긴급·돌발 상황 발생 등에 따른 현장 혼잡 최소화를 위한 절차를 마련하고 이에 대한 내용을 기술

❍ 개인정보 유출등 사고 대응팀은 O층 OO회의실에 오프라인 창구를 개설

- 전화, 메일, 홈페이지, SNS 등 한 가지 이상의 채널을 선택하여 단일화된 민원 대응 창구를 구축

구분	채널	상세 내용(예시)
오프라인	0층 00회의실	
온라인 中 택 1	전화	055-000-0000
	메일	ooooo@ooo.ooo
	홈페이지	https://ooo.gnu.ac.kr
	SNS	#OOOO

❍ 정보주체가 개인정보 유출 여부 등을 확인 가능하도록 별도의 홈페이지 등을 제공

※ 개인정보 유출 결과는 전체 공지가 아닌 핸드폰 인증 등을 통해 정보주체가 개별 본인 확인 후 개인정보 유출 결과 조회 지원

❍ 복구반은 유출등이 된 시스템의 이용을 제한하고 별도의 임시 시스템 구축을 통하여 기관의 업무 혼잡 방지

※ 현장에서 물리적 시스템 장애, 파괴 그리고 불필요한 인력 등으로 인하여 개인정보가 분실, 도난, 훼손되지 않도록 주의

❍ 분석반은 대외 수사기관에 협조할 수 있는 전담 인력 구성 및 대응

❍ 시스템 오류 등 서비스 장애로 인한 정보주체의 민원 발생 시 유관부서와 협의하여 해결

2.4 정보주체 민원 대응조치

가이드

o 개인정보처리자는 정보주체 민원을 처리할 수 있는 체계를 만들고 이에 대한 내용을 기술

- ❍ 민원대응반은 유관부서(정부, 언론사, 이용자 민원 대응)와 협의하여 피해자 구제 방안, 수사 진행 상황 등에 대한 외부 질의 답변 방향 결정
- ❍ 협의 방안을 토대로 민원 대응 매뉴얼 작성 및 배포
- ❍ 민원 대응 전담 인력·회선 확보 및 대응 매뉴얼 교육
- ❍ 대외적 접촉 창구는 민원대응반으로 단일화하여 부서 및 대민 OOO 홈페이지(http://ooo.com)에 공지하고 타 팀에서 외부로부터 개인정보 유출등 관련 질문을 받으면 최대한 민원대응반으로 연결
- ❍ 기본적으로 민원대응반을 통해서 1차 민원 대응을 하되, 별도 대응이 필요한 경우 해당 부서에서 응대하도록 안내

문의별	담당부서
유출 확인 문의 대응	부서 담당자
피해구제 관련 문의 대응	감사팀 민원대응반
기타	부서 개인정보담당자

2.5 정보주체 불안 해소 조치

가이드

o 개인정보처리자는 정보주체가 유출등이 된 개인정보로 인한 불안을 해소할 수 있는 체계를 마련하고 이에 대한 내용을 기술

- ❍ OOO홈페이지(http://ooo.com)에 유출등 피해 최소화를 위해 현재 기관에서 실시하고 있는 노력에 대한 사항 공지(1일 1회 이상 업데이트)

❍ 비밀번호, 신용카드번호 등 유출 시 비밀번호 변경, 카드 재발급 등을 할 수 있도록 유출통지 시 함께 안내

※ 불법스팸대응센터(☏118, spam.kisa.or.kr)를 통하여 불법스팸신고 및 차단 등을 구체적으로 안내

[개인정보 유출 항목별 2차 피해 예방을 위한 안내사항]

항목	세부 안내 사항
아이디, 비밀번호	- 비밀번호 변경 안내
카드번호	- 카드 재발급 절차 안내
다량의 개인정보	- 보이스피싱 등 2차 피해 예방 안내

❍ (정보주체 요청이 있을 시) 회원 탈퇴 방법 안내 및 정보주체의 개인정보 삭제 조치

2.6 피해자 구제 조치

가이드

o 개인정보처리자는 정보주체가 피해를 구제할 수 있는 절차를 마련하고, 이에 대한 내용을 기술

❍ 정보주체에게 개인정보 유출등 피해에 대한 피해구제, 상담 등을 문의할 수 있음을 안내

❍ 개인정보를 유출당한 사람은 누구든지 개인정보 분쟁조정위원회에 분쟁조정을 신청할 수 있음을 안내(「개인정보 보호법」 제43조제1항)

❍ 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있음을 안내

3 개인정보 유출등 원인별 보호 조치

3.1 해킹에 의한 경우

❍ 개인정보가 유출된 사실을 알게 된 경우에는 개인정보 추가 유출 방지를 위한 대책을 마련하고 피해를 최소화할 수 있는 조치를 강구 하여야 함

- 유출된 시스템 분리·차단 조치, 관련 로그 등 증거자료 확보, 유출 원인분석, 이용자 및 개인정보취급자 비밀번호 변경* 등 기술적 보호 조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 긴급 조치를 시행하여야 함

  * 일방향 암호화되지 않은 비밀번호가 유출되었거나, 해커 등이 이용자의 비밀번호를 알고 있다고 판단되는 경우에는 이용자가 비밀번호를 변경하지 않으면 이용할 수 없도록 하고, 일방향 암호화된 비밀번호가 유출된 경우에도 비밀번호 변경을 유도하여 추가 피해 예방 방지

- 사고 원인 조사 등 조치가 완료된 이후에는 개인정보 유출의 직·간접적인 원인을 즉시 제거하고, 미비한 보호조치 부분을 파악하기 위한 취약점 점검·개선 조치 등을 수행하여야 함

3.2 내부자 유출

❍ 개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보 열람·다운로드 등 내역을 확인하여야 함

❍ 개인정보 유출자의 개인정보처리시스템에 대한 접근·접속 경로 등을 확인하고, 비정상적인* 접속인 경우 접속경로를 확인하여 차단하여야 함

  * 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드·삭제·출력 등

❍ 개인정보취급자의 개인정보처리시스템 접속 계정, 접속 권한, 접속 기록 등을 검토하여 추가적인 유출 여부를 확인하여야 함

❍ 개인정보 유출에 활용된 단말기(PC, 스마트폰 등)와 매체(USB, 이메일, 출력물 등)를 회수하고, 필요시 수사기관 등과 협조하여 유출된 개인정보를 회수하기 위한 모든 방법을 강구 하여야 함

3.3 이메일 오발송에 의한 경우

❍ 이메일 회수가 가능한 경우에는 즉시 회수 조치하고, 불가능한 경우에는 이메일 수신자에게 오발송 메일의 삭제를 요청*하여야 함

* 삭제 요청 시 가능한 삭제 되었음을 확인할 수 있는 증빙자료 첨부를 같이 요청(예: 삭제 전 목록화면과 삭제 후 목록화면을 받음)

❍ 메일서버 외 첨부파일 서버(대용량 메일 등)를 이용하는 경우 첨부파일 서버 운영자에게 관련 파일의 삭제를 요청하여야 함

3.4 개인정보 노출

❍ **(외부 검색엔진을 통한 노출의 경우)** 노출된 사업자의 웹페이지 삭제를 검토하고, 검색엔진에 노출된 개인정보 삭제를 요청하여야 하며, 필요시 로봇 배제 규칙*을 적용하여 외부 검색엔진의 접근을 차단하여야 함

* 홈페이지 공개 원칙에 벗어나지 않는 범위 내에서 로봇 배제 적용 필요

❍ **(관리자 페이지에 접속하여 노출된 경우)** 관리자의 접속 IP를 제한하고, 소스코드를 수정하여 사용자 인증 절차를 추가하여야 함

❍ **(개인정보취급자 부주의로 인한 노출의 경우)** 게시글 및 첨부파일 내 개인정보 노출 부분을 삭제 또는 마스킹 처리하여 필요한 경우 다시 게시하여야 함

❍ **(상용 오피스 취약점으로 노출된 경우)** S/W버전은 항상 최신버전*으로 이용하며 홈페이지 첨부파일 탑재 시 엑셀 문서는 PDF 등으로 변환**하여 탑재

* 엑셀2003 이하에서는 외부 링크 취약점이 존재하여 엑셀2007 이상 버전 사용 (관련 문서: 교육부 교육정보화과-4027(2017.08.04.))

** 엑셀은 OLE개체, 열·행·시트 숨김, 치환함수, 피벗테이블 등의 다양한 기능으로 사용자가 인지하지 못하는 개인정보 등 노출 발생 가능성 높음

4 개인정보 유출등 사고 재발방지 조치

4.1 유출등 원인 보완 및 재발 방지 조치계획 수립·이행

❍ 개인정보 유출등 원인별 긴급 보호조치를 취한 이후 보완 대책 점검 및 보완 실시

❍ 중장기 보완 대책을 위해 재발 방지 계획을 수립하고 수립된 계획에 따라 이행 실시*

* 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호)에 따라 개인정보보호 책임자가 내부관리계획의 이행 실태를 연 1회 이상 점검·관리할 때 이행 여부 점검 권고

4.2 재발 방지 교육 및 사례전파

❍ 대학 내 구성원 재발 방지 교육 실시

- 개인정보 유출등과 관련된 부서 내 모든 취급자는 필수적으로 재발 방지 교육 실시

❍ 개인정보 유출등 사례를 내부 공지 등을 통해 기관 내 구성원에게 사례를 전파*

* 사례전파 시 또 다른 개인정보 유출등이 발생하지 않도록 주의 필요

- 사례전파의 구성(예시)

구분	구성 내용
사고 개요	• 0년 0월 0일 개인정보 취급자가 홈페이지 게시판 관리 중 개인정보가 포함된 파일을 게시판에 탑재함 • 개인정보가 포함된 파일(엑셀)을 00으로부터 0년 0일 0일 인지하여 해당 파일 삭제 조치함 • 개인정보 00건, 포함된 개인정보 항목은 00을 포함한 총 00개가 유출됨
사고 처리 절차	• 정보주체에게 유출 통지를 하였으며, 홈페이지에 관련 내용을 탑재하여 전파 • 피해구제 방안 등 정보주체 민원대응반 구축 • 재발방지대책(교육 등)을 수립
대학 보완 조치 내용	• 개인정보 취급자 대상 개인정보 교육 실시 • 개인정보 웹 필터링 시스템 도입으로 개인정보 파일 검출 • 대학 개인정보 체계 강화를 위한 홍보자료 및 사례 전파 실시
향후 대학의 보완 방향	• 개인정보 필터링 시스템 등 개인정보 체계 강화를 위한 시스템 구축 • 매년 개인정보 취급자 대상 개인정보 교육 실시
관련 변경 지침	• 내부 관리계획 수립 시 개인정보 유출등 재발 방지 계획 포함

붙임1 **개인정보 유출등 신고서(양식)**

개인정보 유출등 신고서

기관명					
유출등이 된 개인정보 항목 및 규모					
유출등이 된 시점과 그 경위					
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등					
개인정보처리자의 대응조치 및 피해 구제절차					
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처					
유출등 신고(보고) 담당자		성명	부서	직위	연락처
	개인정보 보호책임자				
	담당자 (취급자)				

유출등 신고 접수기관	기관명	담당자명	연락처

개인정보 유출등 신고서(작성 사례)

<table>
<tr><td>기관명</td><td colspan="5">0000000</td></tr>
<tr><td>유출등이 된
개인정보 항목 및
규모</td><td colspan="5">▪ 유출 규모: 1,150명(중복제거 후 1,100명)
- 교육부 신고(2024.3.22. 13:00), 개인정보위 신고여부(2024.3.22. 12:00)
▪ 유출 항목: 이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일</td></tr>
<tr><td>유출등이 된 시점과
그 경위</td><td colspan="5">▪ 사고 발생 인지 경위(인지 시점 포함)
- 2024.3.21 10:00 월별 개인정보처리시스템 접속 로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인
- 2024.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견
- 2024.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인
▪ 유출 시점 및 경위
- 2024.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드
- 2024.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송</td></tr>
<tr><td>유출등 피해
최소화를 위해
정보주체가 할 수
있는 방법 등</td><td colspan="5">▪ 정보주체가 할 수 있는 피해 최소화 방법
① 2차 피해 방지를 위하여 개인정보 유출 여부 조회(학교 홈페이지 등)
② 유출사고 발생 후 홈페이지 로그인시 개인정보 유출에 따른 비밀번호 변경
▪ 사고 발생 후 조치 사항
① 기관 개인정보 유출사고 대응 매뉴얼에 따라 유출사고 대응반 구축
② 개인정보 유출 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 재발 방지 대책을 위한 보안 강화계획(안) 수립</td></tr>
<tr><td>정보주체에게 피해가
발생한 경우 신고
등을 접수할 수 있는
담당부서 및 연락처</td><td colspan="5">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)</td></tr>
<tr><td rowspan="3">정보주체에게 피해가
발생한 경우 신고
등을 접수할 수 있는
담당부서 및 연락처</td><td></td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보
보호책임자</td><td>김영희</td><td>총무과</td><td>총무과장</td><td>055-123-1234</td></tr>
<tr><td>개인정보
취급자</td><td>홍길동</td><td>총무과</td><td>담당자</td><td>055-123-1234</td></tr>
</table>

유출등 신고 접수기관	기관명	담당자명	연락처
	한국교육학술정보원 및 교육부	김철수	055-234-5678

붙임2 **개인정보 유출등 신고 조치확인서(양식)**

개인정보 유출등 신고 조치확인서(양식)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성(moeprivacy@keris.or.kr로 제출).

<table>
<tr><td colspan="2">기관명</td><td>00000학교</td></tr>
<tr><td rowspan="3">정보주체
통지 여부</td><td>통지일시</td><td>2024.00.00. 12:00</td></tr>
<tr><td>통지방법</td><td>(예시) 전화, 이메일, 서면, 팩스, 홈페이지 공개* 등
* 정보주체의 연락처를 알 수 없는 경우</td></tr>
<tr><td>필수통지
항목</td><td>
<table>
<tr><th>필수 통지 항목 5가지</th><th>포함 여부 확인(O, X)</th></tr>
<tr><td>① 유출등이 된 개인정보의 항목</td><td>O 또는 X</td></tr>
<tr><td>② 유출등이 된 시점과 및 그 경위</td><td>O 또는 X</td></tr>
<tr><td>③ 피해 최소화를 위한 정보주체가 할 수 있는 방법</td><td>O 또는 X</td></tr>
<tr><td>④ 기관의 대응조치 및 피해구제 절차</td><td>O 또는 X</td></tr>
<tr><td>⑤ 피해 신고·상담 부서 및 연락처 등</td><td>O 또는 X</td></tr>
</table>
(예시) 이메일, 팩스, 홈페이지 공개 등 내용 이미지 캡쳐 등 증빙자료 포함
</td></tr>
<tr><td colspan="2">발생(인지) 일자</td><td>2024.00.00.</td></tr>
<tr><td colspan="2">발생(인지) 경로</td><td>(예시)
- 2024.00.00 00:00 KISA에서 통보
- 정보주체가 해당 학과에 신고, ECSC 사고 신고, 민원인 신고 등</td></tr>
</table>

<table>
<tr><td>유출등 사실 인지 이후 후속 조치 경과
(유출등 피해 최소화 대책·조치 및 결과)</td><td colspan="3">개인정보 유출등 발생시 아래 사항 준수
1. 개인정보 유출등 대응 매뉴얼 구비
※ 법령에 기반하여 최신화 되어있는지 확인 및 개선, 유출등 발생시 매뉴얼대로 즉시 신고 등 대응
2. 유출등 원인 보완 및 재발 방지 조치계획 수립·이행
3. 개인정보취급자(전직원) 대상 사례 전파 및 재발 방지 교육
※ 개인정보보호 관련 전 직원 교육 실시, 특히 신규 직원은 업무 투입 전 개인정보보호 기본 교육 실시 후 투입
4. 그 밖의 개인정보의 유출등 방지를 위해 필요하다고 판단되는 사항

(예시)
- 2024.00.00 00:00 해당 게시글 삭제
- 2024.00.00 00:00 정보주체에게 메일, 문자로 안내
- 2024.00.00 00:00 홈페이지취약점 점검 수행
- 2024.00.00 00:00 00홈페이지에 유출 건 내용 게시
- 2024.00.00 00:00 재발방지대책 수립
- 2024.00.00 00:00 전 직원 대상 개인정보 관련 교육
- 개인정보 파일 삭제, 오발송된 이메일 회수, 사례전파, 교육 실시 등 증빙자료 포함</td></tr>
<tr><td>교육부 신고 일시
(1명 이상 유출등)</td><td>2024. 0. 00. 12:00</td><td colspan="2">[교육부 신고]
유출등 통지 및 조치 결과를 지체없이 상급 기관을 경유하여 교육부에 신고(교육부 개인정보보호 포털(privacy.moe.go.kr)</td></tr>
<tr><td>개인정보보호위원회 신고 일시
(1천명 이상,
민감정보·고유식별정보,
외부로부터의 불법적인 접근으로 유출등)</td><td>2024. 0. 00. 12:00</td><td colspan="2">[교육부 및 개인정보보호위원회 신고]
유출등 통지 및 조치 결과를 지체없이 상급 기관을 경유하여 교육부에 신고하고(교육부 개인정보보호 포털), 개인정보보호위원회(또는 한국인터넷진흥원, www.privacy.go.kr)에 신고</td></tr>
<tr><td rowspan="2">유출등이 된
개인정보</td><td>규모(명)</td><td>00명</td><td>(중복제거) 00명</td></tr>
<tr><td>항목</td><td colspan="2">이름, 핸드폰번호 ,,,,,</td></tr>
<tr><td>유출등이 된 시점과 그 경위</td><td colspan="3">(예시)
- 2024.00.00 00:00 메일 잘못 발송, 실수로 개인정보 파일 첨부함
- 2024.00.00 00:00 유출 확인</td></tr>
</table>

정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	(예시) 피해구제절차 안내 등
진행사항 또는 향후계획	(예시) 자체 내부 감사 수행, 상위기관 현장 컨설팅 수행, 개인정보보호위원회 점검 예정 등

※ 유출등 신고 후 1주일 이내 조치 확인서를 작성하여 교육부 개인정보보호 포털-유출신고 내역을 수정하여 제출하거나 메일(moeprivacy@keris.or.kr)로 반드시 제출

개인정보 유출등 신고 조치 확인서(작성 사례)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성(moeprivacy@keris.or.kr로 제출).

<table>
<tr><td colspan="2">기관명</td><td>경상국립대학교</td></tr>
<tr><td rowspan="3">정보주체
통지 여부</td><td>통지일시</td><td>2024. 3. 22. (화) 13:00</td></tr>
<tr><td>통지방법</td><td>이메일 및 유선 전화</td></tr>
<tr><td>필수통지
항목</td><td>
<table>
<tr><th>필수 통지 항목 5가지</th><th>포함 여부 확인(O, X)</th></tr>
<tr><td>① 유출등이 된 개인정보의 항목</td><td>O</td></tr>
<tr><td>② 유출등이 된 시점과 및 그 경위</td><td>O</td></tr>
<tr><td>③ 피해 최소화를 위한 정보주체가 할 수 있는 방법</td><td>O</td></tr>
<tr><td>④ 기관의 대응조치 및 피해구제 절차</td><td>O</td></tr>
<tr><td>⑤ 피해 신고·상담 부서 및 연락처 등</td><td>O</td></tr>
</table>
개인정보 유출 사실을 통지해 드리며,
깊이 사과 드립니다.

고객님의 개인정보는 2023년 3월 4일 00용역업체 직원에 의하여 외부 유출된 사실을 확인하였고, 2차 피해 예방을 위해 경찰청에 즉시 조사를 의뢰하여 수사진행 중입니다.

유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 핸드폰번호, 주소 총 6개 항목입니다.

유출 사실을 인지한 후 즉시 접속 경로를 차단하고, 취약점 점검과 보완 조치를 완료 하였습니다.

현재까지 확인한 바로는 경찰청에서 00용역업체 직원이 외부로 유출된 개인정보는 제3자에게 2차 전달하거나 판매하지 않는 것으로 확인 되었습니다.

혹시 모를 피해를 최소화하기 위하여 00시스템과 동일한 ID 및 비밀번호를 사용하고 있는 웹사이트가 있다면, 귀하의 계정정보(ID/비밀번호)를 변경하여 주시기 바랍니다.

아울러 피해가 발생하였거나 기타 궁금하신 사항은 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조치를 거쳐 손해배상 등의 구제절차를 진행하도록 하겠습니다.

앞으로 해당 서비스에 대한 보안 및 개인정보보호 조치 강화 등 개인정보에 대한 관리체계를 개선하고, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.

귀하께 심려를 끼쳐 드리게 되어 거듭 진심으로 사과 드립니다.

▶ 피해 등 접수 담당부서: 0000팀(00-0000-0000)
▶ 피해 등 접수 메일:0000@0000.kr

00교육기관 000
</td></tr>
</table>

<table>
<tr><td colspan="2">발생(인지) 일자</td><td colspan="3">2024.3.21.</td></tr>
<tr><td colspan="2">발생(인지) 경로</td><td colspan="3">- 2024.3.21 10:00 월별 개인정보처리시스템 접속로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인
- 2024.3.21 10:30 정보보안 솔루션(방화벽, IPS 등) 로그 분석 결과 외부 해킹 공격은 없음
- 2024.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견
- 2024.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인
- 2024.3.21 13:00 해당 PC 점검 및 유출 내용 확인</td></tr>
<tr><td colspan="2">유출등 사실인지 이후 후속 조치 경과
(유출등 피해 최소화 대책・조치 및 결과)</td><td colspan="3">- 2024.3.21. 12:00 기관 개인정보 유출사고 대응 매뉴얼에 따라 유출사고 대응반 구축
- 2024.3.21. 13:30 개인정보 유출 접수 창구 및 민원 대응 창구 구축
- 2024.3.21. 14:00 유출 항목 및 발생 상황 인지 후 유출 통지문 작성 및 관련 내용 통지, 개인정보보호위원회 및 교육부 개인정보 유출 신고
- 2024.3.21. 14:30 유출 원인에 따른 개인정보처리시스템에 대한 접근권한 관리체계 강화
- 2024.3.21. 15:00 유출 피해 최소화를 위해 추가 확인 정보 공지 및 관련 내용 현행화 실시
- 2024.3.21. 15:30 재발방지 대책을 위한 보안강화 계획(안) 수립
1) 보안 솔루션 도입
2) 전 직원 대상 사례전파 교육 및 개인정보 교육
3) 모든 개인정보처리시스템 대상 안전성 확보 조치 방안 점검</td></tr>
<tr><td colspan="2">교육부 신고 일시
(1명 이상 유출등)</td><td>2024. 3. 22. 14:00</td><td colspan="2">[교육부 신고]
유출등 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고(교육부 개인정보보호 포털(privacy.moe.go.kr)</td></tr>
<tr><td colspan="2">개인정보보호위원회 신고 일시
(1천명 이상,
민감정보·고유식별정보,
외부로부터의 불법적인 접근으로 유출등)</td><td>2024. 3. 22. 14:00</td><td colspan="2">[교육부 및 개인정보보호위원회 신고]
유출등 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고하고(교육부 개인정보보호 포털), 개인정보보호위원회(또는 한국인터넷진흥원, www.privacy.go.kr)에 신고</td></tr>
<tr><td rowspan="2">유출등이 된
개인정보</td><td>규모(명)</td><td colspan="2">1,150명</td><td>(중복제거) 1,100명(학생 600명, 학부모 200명, 교직원 300명)</td></tr>
<tr><td>항목</td><td colspan="3">이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일</td></tr>
<tr><td colspan="2">유출등이 된 시점과 그 경위</td><td colspan="3">- 2024.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드
- 2024.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송</td></tr>
</table>

정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차	▪ 정보주체가 할 수 있는 피해 최소화 방법 ① 2차 피해 방지를 위하여 개인정보 유출 여부 조회(학교 홈페이지 등) ② 유출사고 발생 후 홈페이지 로그인 시 개인정보 유출에 따른 비밀번호 변경 ▪ 피해자 구제 절차 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)
진행사항 또는 향후 계획	① 개인정보 파일 운영 강화를 위한 보안 솔루션 도입(DLP, DRM 등) ② 용역업체(유지보수 등)가 접속할 수 있는 별도의 계정 생성 ③ 개인정보취급자 대상 개인정보보호 교육 강화 ④ 모든 개인정보처리시스템 대상 개인정보 보호법 등 관련 법률에 따라 개인정보 안전성 확보 조치 이행 사항 확인 및 관련 내용 점검

※ 유출등 신고 후 1주일 이내 조치확인서를 작성하여 교육부 개인정보보호 포털-유출 신고 내역을 수정하여 제출하거나 메일(moeprivacy@keris.or.kr)로 반드시 제출

붙임3 개인정보 유출등에 따른 2차 피해 유형 및 대응 요령

	피해 종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응 요령
금전적	온라인 사기 쇼핑	주민등록번호, 카드번호, 유효기간 등	① 카드번호, 유효기간으로 온라인 결제가 가능한 국내외 홈쇼핑 사이트에 접속 ② 홈쇼핑 홈페이지, ARS를 통한 온라인 사기 결제·주문	• 신용카드 정지 및 재발급 신청 ※ 신고기관 : 각 카드사, 한국소비자원 소비자 상담센터(☏1372) 등
	명의도용을 통한 통신서비스 가입	이름, 주소, 주민등록번호 등	① 유출된 개인정보를 이용하여 휴대전화, 인터넷전화 등 가입 ※ 통신서비스 가입 시 본인 확인 절차가 있으므로 주민등록증 위조 등 추가적인 불법 행위 수반이 예상됨 ② 불법 가입한 전화번호로 스팸을 발송하여 금전적 이익을 취득함 ※ 명의를 도용당한 사람은 서비스 이용 제한을 당하거나 명의도용 소명 절차를 밟는 등 피해를 당함	• 한국정보통신진흥협회(KAIT)의 명의도용방지서비스(M-Safer)를 통한 불법 통신서비스 신규 가입 여부 확인 ※ 신고기관 : 통신민원조정센터(msafer.or.kr) ※ 명의도용방지서비스(M-Safer) : 통신서비스 신규 가입 시 이메일·문자로 가입 여부 통보
	명의도용을 통한 신용카드 복제	이름, 신용카드 번호, 유효기간 등	① 유출된 개인정보를 이용하여 신용카드 불법 복제 ※ 특수장비를 이용하여 카드번호, 유효기간, 이름 등으로 복제 가능 ② 불법 복제된 카드를 국내외에서	• 신용카드 정지 및 재발급 신청, 이용 내역 통지 서비스 가입 ※ 신고기관 : 각 카드사, 경찰, 금융감독원(☏1332)

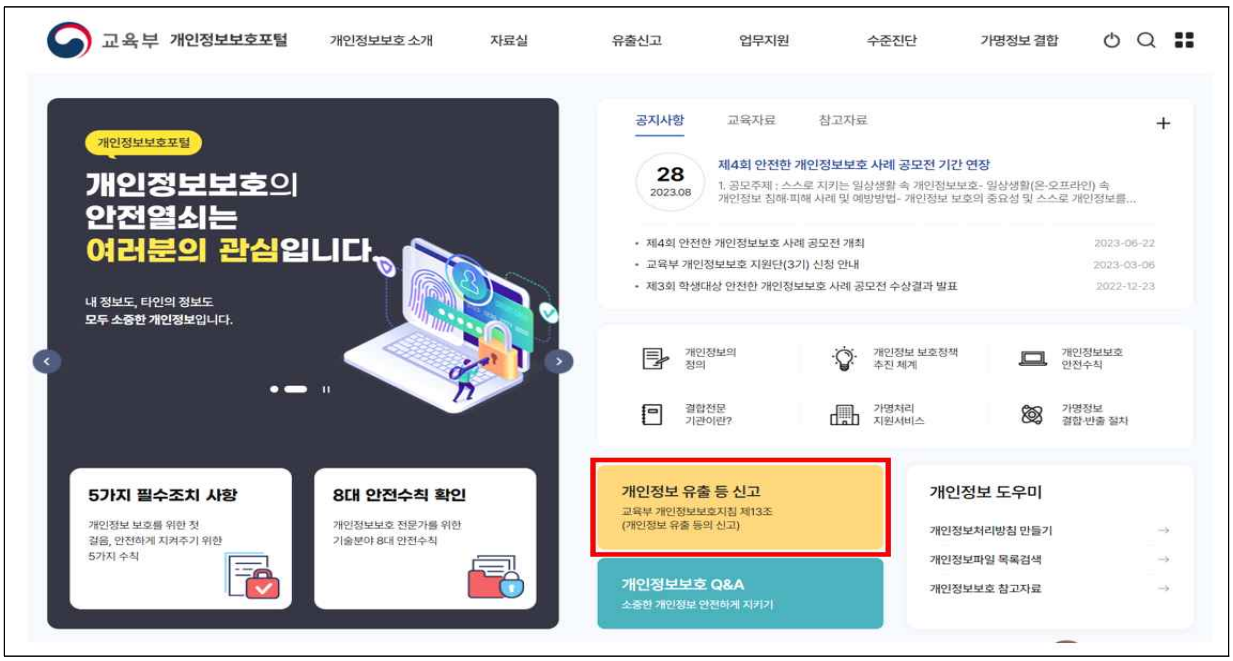
	피해 종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응 요령
			활용하여 상품 결제 등에 악용 ※ 국내외 POS단말기의 경우 마그네틱 부분만을 이용하여 결제 가능	
	스미싱	휴대전화번호	① '정보유출 확인 안내' 등 금융기관을 사칭 하는 문자메시지에 악성코드(인터넷주소)를 삽입하여 발송 ② 금융기관 사칭 메시지를 받은 피해자가 인터넷주소(URL)를 클릭하면 악성코드에 감염되어 소액결제 피해 및 개인·금융정보 탈취	• 수상한 문자메시지 삭제 및 메시지 상 링크 클릭하지 않기 또는 카드사 공지 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☏118)
비금전적	보이스피싱	신용카드번호, 휴대전화, 집전화번호, 집주소 등	① 경찰, 금융감독당국 또는 금융회사 직원을 사칭하여 전화 ② 금융관련 업무 목적 사칭을 통한 개인정보·금융정보 탈취(비밀번호, 보안카드번호 등) ③ 유출된 금융사를 사칭, 개인정보 유출 확인을 빙자하여 ARS를 통해 계좌번호/비밀번호 등 금융정보 입력 요청	• 수상한 전화 거부 및 각 카드사에서 공지한 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☏118)
	명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름,	• e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청 ※ 신고기관 : 경찰, 불법스팸대응센터(☏118)

	피해 종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응 요령
			이메일, 연락처만으로 회원가입 가능 ② 명의도용을 통해 본인도 모르는 수십여개의 웹사이트 가입하여 개인정보 불법 이용	※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 미사용시 서비스 불가
	휴대전화/이메일 스팸 발송	휴대전화 번호, 이메일 주소 등	① 유출된 개인정보를 이용해 불특정 다수에게 스팸 발송 ※ 유출된 모든 휴대전화, 이메일로 도박 등 스팸 무작위 발송 가능 ※ 신용정보, 연소득등 활용 대출 스팸 발송, 자동차 보유 여부를 활용한 보험 스팸 발송 등 특정유형의 개인에 대한 타겟 마케팅 가능 ② 휴대전화, 이메일 서비스 이용자는 원치 않는 홍보·마케팅 광고 수신	• 지능형 스팸 차단서비스를 이용한 스팸 차단, 수신 스팸 적극 신고 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☏118) ※ 지능형 스팸 차단 서비스 : 발신·회신번호 등 발송패턴을 분석하여 스팸을 차단 해주는 서비스
	사회공학적 기법을 활용한 악성코드 유포 메일 발송	이메일 주소 등	① 해커가 특정 대상을 목표로 스팸/피싱 시도용 첨부파일이 포함되어 있거나 연결을 유도 URL이 포함된 이메일 발송 ② 수신자들이 이메일에 포함된 첨부파일 및 URL을 클릭 ③ 해커가 수신자의 PC를 장악하여 기밀 및 개인정보를 빼냄	• 의심 가는 이메일을 받은 경우 함부로 열람하지 않고 바로 삭제 • 사용자 PC의 바이러스 백신을 항상 최신버전으로 유지 및 정기적 검사 수행 ※ 신고기관 : 경찰, 불법스팸대응센터(☏118)

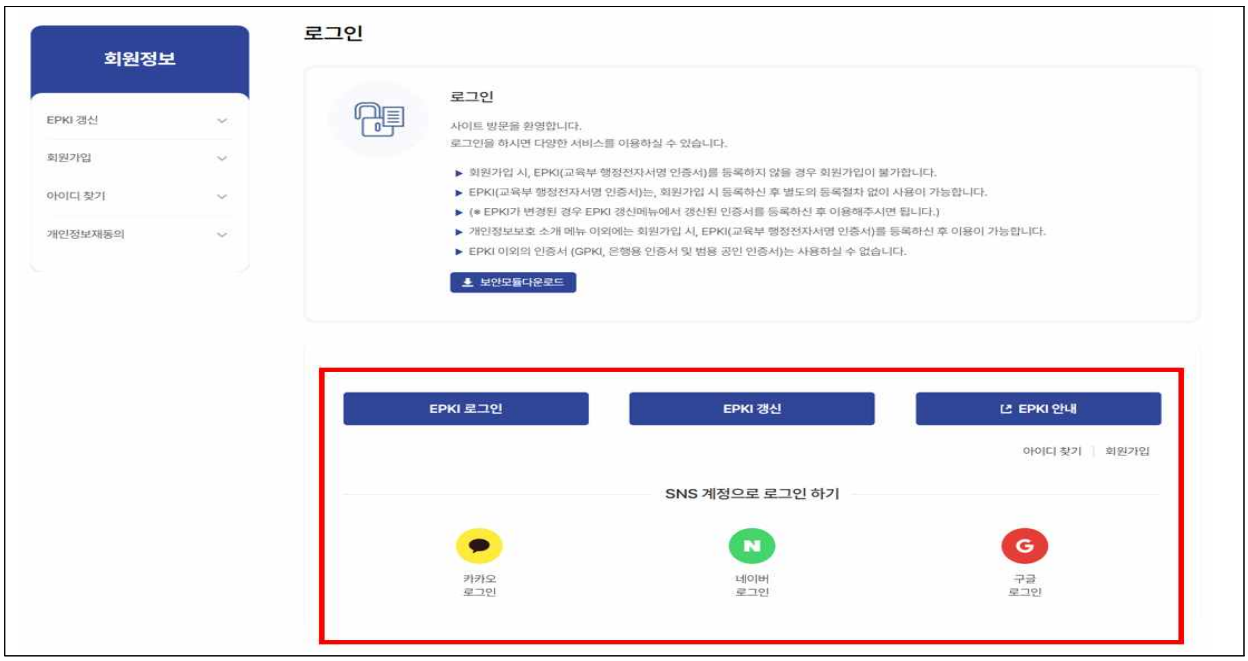
붙임4 교육부 개인정보보호 포털 유출등 신고 절차

▢ 유출등 신고 절차

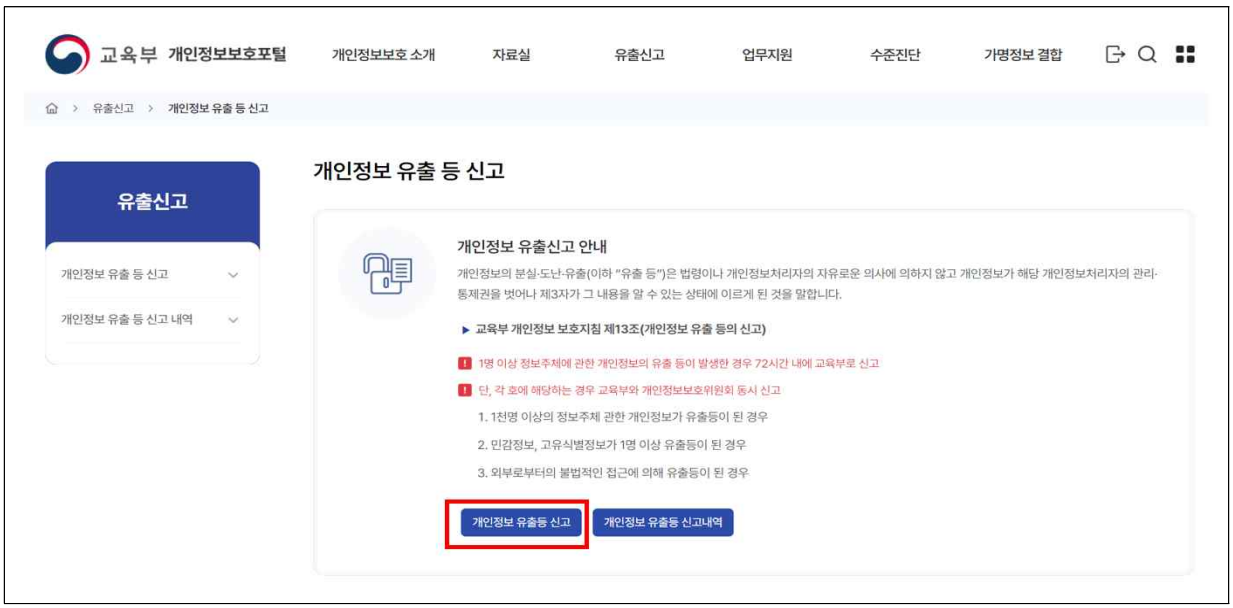
[1단계] 교육부 개인정보보호 포털(https://privacy.moe.go.kr) 사이트 접속 →
① [개인정보 유출 등 신고] 선택



[2단계] EPKI 로그인 및 SNS(카카오, 네이버, 구글) 계정으로 로그인 실시

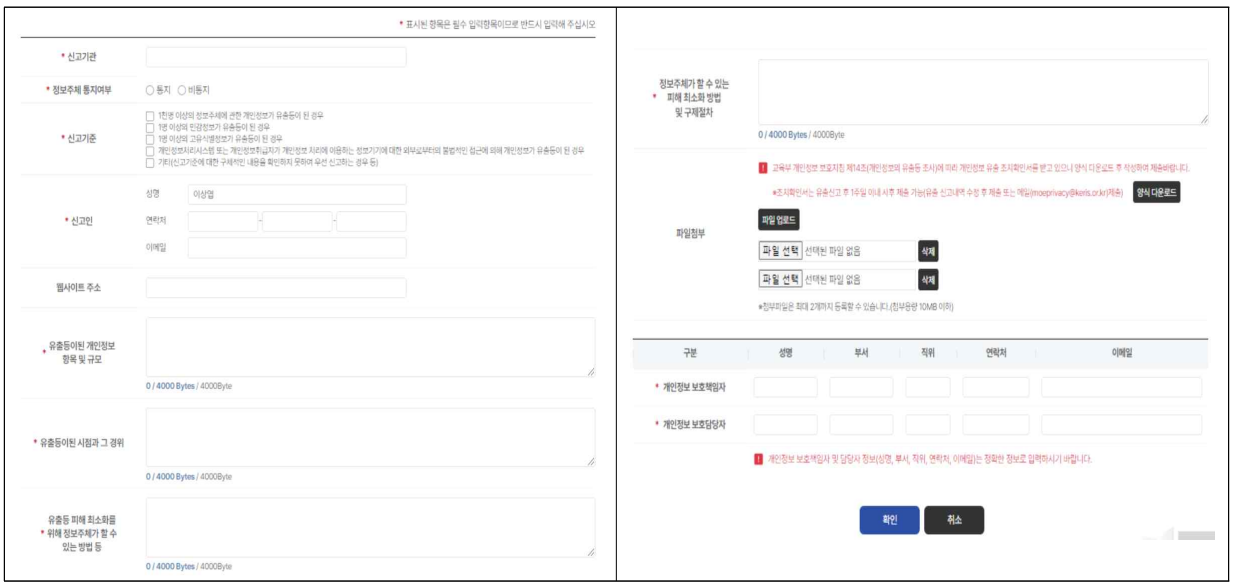


[3단계] ① [개인정보 유출등 신고] 선택



[4단계] ① [유출신고 관련 내용 작성] → ② [확인] 완료

※ 유출등 신고서 내용은 정확한 정보(이메일, 연락처 등)로 입력하여 작성

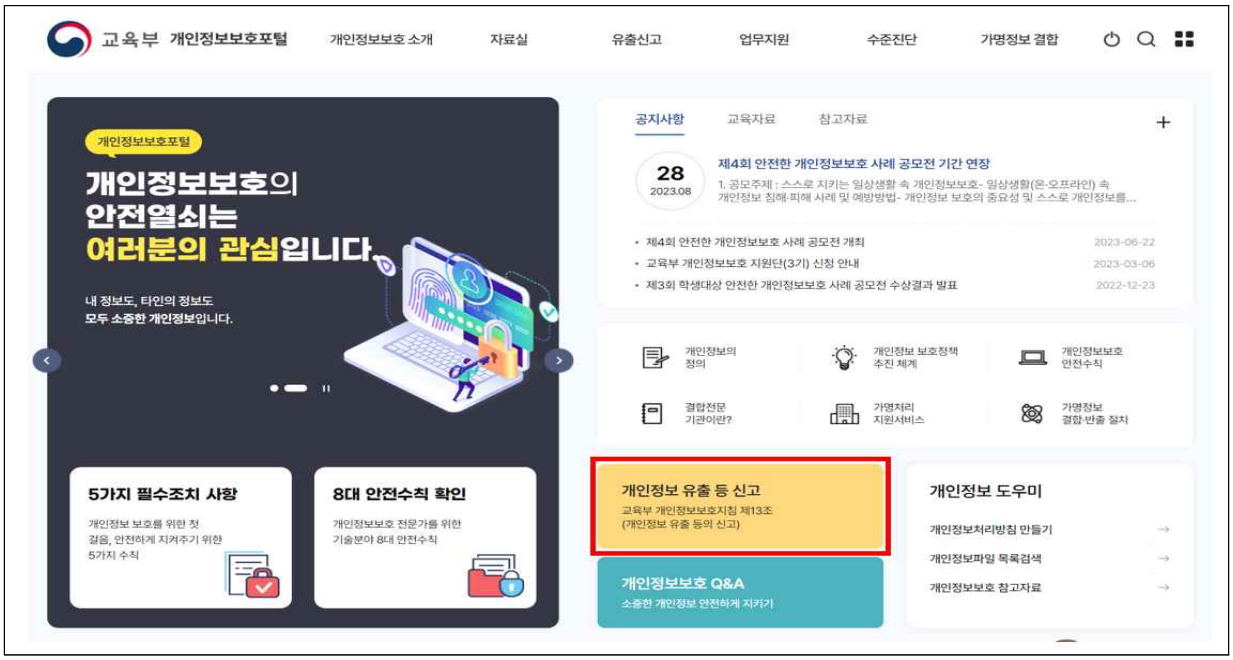


[5단계] 교육부 개인정보 보호지침 제13조에 따른 개인정보 유출 등 신고서(붙임1)를 첨부파일로 제출

※ 개인정보 유출 등 신고 완료 후 1주일 이내 개인정보 유출등 신고 조치 확인서(붙임2)를 작성 후 교육부 개인정보보호 포털-유출신고 내역 수정하여 제출하거나 메일(moeprivacy@keris.or.kr)로 전달

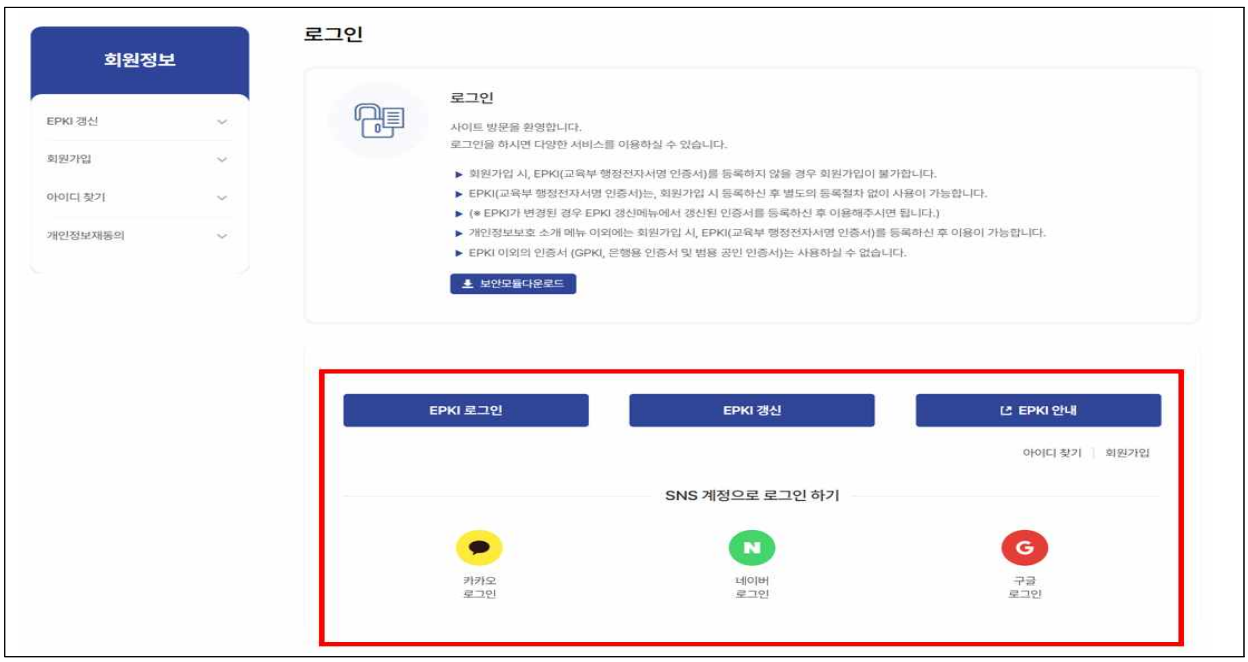
▢ 유출등 신고 내역 수정(조치확인서 제출 등) 절차

[1단계] 교육부 개인정보보호 포털(https://privacy.moe.go.kr) 사이트 접속 →
① [개인정보 유출 등 신고] 선택

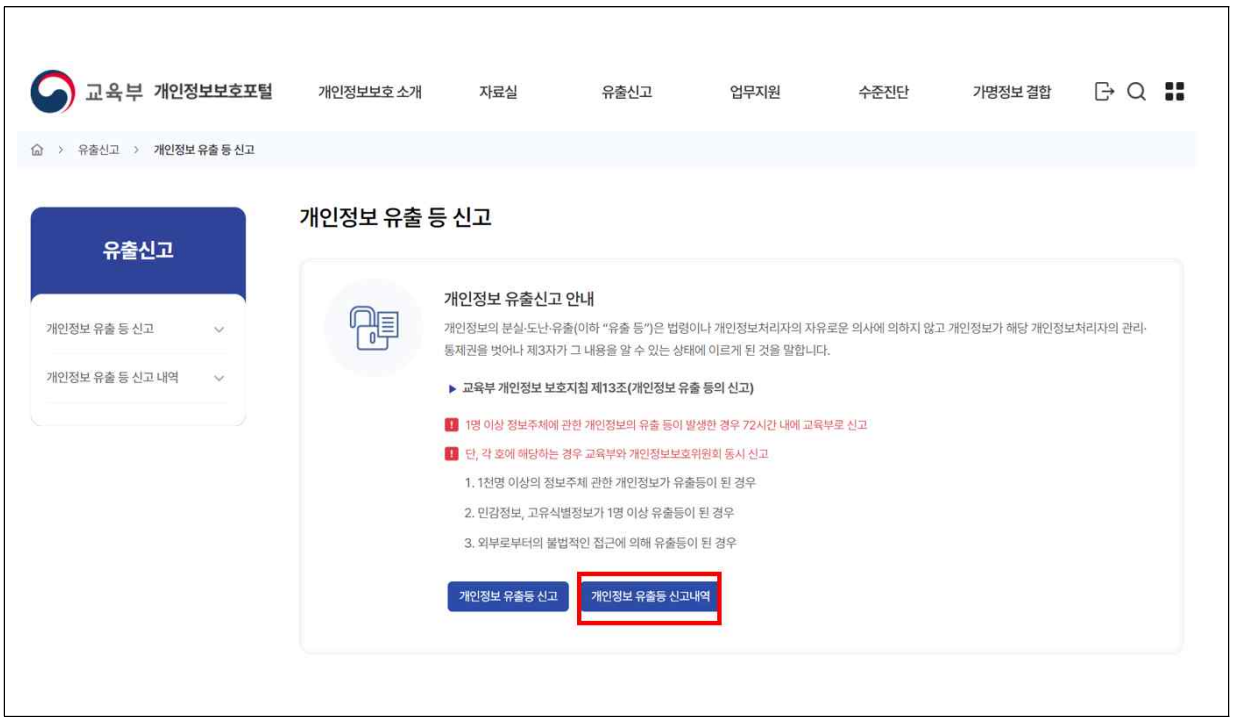


[2단계] EPKI 로그인 및 SNS(카카오, 네이버, 구글) 계정으로 로그인 실시

※ 개인정보 유출등 신고한 계정과 동일 계정으로 로그인(동일한 계정 아닐 경우 수정 불가)



[3단계] ① [개인정보 유출등 신고 내역] 선택



[4단계] ① 유출등 신고 내역 확인 후 수정할 유출등 신고 내역 선택

[5단계] ① [수정] 선택 후 내용 수정

[6단계] ① 유출등 신고 내역 수정 후 [확인] 선택

※ 개인정보 유출등 신고서(붙임1), 개인정보 유출등 신고 조치 확인서(붙임2)를 작성하여 붙임파일로 제출

붙임5 유관기관 관련 연락처

□ 개인정보 유출등 신고

기 관 명	전화번호	인터넷사이트
교육부	-	https://privacy.moe.go.kr/ (교육부 개인정보보호 포털)
개인정보보호위원회 (한국인터넷진흥원)	118	https://privacy.go.kr/ (개인정보보호 포털)

□ 관련기관 연락처

기 관 명	전화번호	인터넷사이트
대검찰청	1301	https://www.spo.go.kr/
경찰청	182	https://ecrm.cyber.go.kr