사립학교교직원연금공단
홈페이지시스템 개인정보 영향평가

영향평가 요약서

2023. 12

(주)씨에이에스(C·A·S)
Computer Assurance Services

개인정보 영향평가 요약본

<table>
<tr><td colspan="2">공공기관명</td><td colspan="6">사립학교교직원연금공단</td></tr>
<tr><td colspan="2">평가기관</td><td>㈜씨에이에스</td><td>평가기간</td><td>2023.09.11.
~
2023.12.15</td><td>평가예산</td><td>☐ 1천만원 미만
☐ 1천만원 이상~3천만원 미만
☐ 3천만원 이상~5천만원 미만
☐ 5천만원 이상~1억원 미만
■ 1억원 이상</td></tr>
<tr><td rowspan="6">평가대상 시스템 개요</td><td>시스템명</td><td colspan="3">홈페이지시스템</td><td>시스템 구축 또는 변경 일정</td><td>2023.06.01~
2023.12.15</td></tr>
<tr><td>추진개요 및 목적</td><td colspan="5">1) 정부의 행정·공공기관 정보시스템 클라우드 전환 정책에 대한 대응 및 공단 대민정보서비스의 안정적 정보자원 통합 기반 마련
2) 단순 기능·성능 개선 위주의 정보시스템 구축·운영에서 벗어나 공단 대민 정보서비스의 수준 향상 및 전문성·효율성·안정성을 갖춘 통합 정보화 운영환경 구축 추진</td></tr>
<tr><td rowspan="4">추진 성격</td><td>대상여부</td><td colspan="2">5만명 이상 민감정보·고유식별정보 처리</td><td>추진예산</td><td>약 1,513,990천원
(VAT포함,추정금액)</td></tr>
<tr><td>추진주체</td><td colspan="2">사립학교교직원연금공단
정보지원실 정보보안팀</td><td rowspan="2">추진유형</td><td rowspan="2">☐ 신규구축
■ 변경(고도화)
☐ 운영</td></tr>
<tr><td>추진근거</td><td colspan="2">기관 자체 필요에 따른 구축</td></tr>
<tr><td>신기술 유형</td><td colspan="3">클라우드 환경으로 전환</td></tr>
<tr><td>주요 내용</td><td colspan="5">○ 대민정보서비스 클라우드 네이티브 전환 설계 및 구현
- 홈페이지시스템의 클라우드 네이티브 전환 설계 및 구현
- 연금서비스, 콜센터 및 VOC시스템 클라우드 전환 기반 마련
- 대민정보서비스 대상 오픈소스DB 구성 및 기존 통합DB와 연계방안 마련
- U2L 전환 및 Web/WAS 공개S/W 전환
- 대민정보서비스 및 VOC 등 관련 기능 개선 및 개발
○ 보안서비스 적용 및 보안성 평가기준 준수
- 보안서비스 적용기준 및 방향
- 보안성 평가기준 준수 등
○ 클라우드 환경에서 문서출력 및 보안관리 기능 도입
- 복합기 및 문서보안
- 내외부망 연동 구성 및 운영서버 이중화</td></tr>
<tr><td>운용체계 변경내용 (변경인 경우)</td><td colspan="5">해당 없음</td></tr>
<tr><td rowspan="2">개인정보파일</td><td>파일명</td><td>정보주체 수</td><td colspan="2">개인정보 항목</td><td>제3자 제공</td><td>개인정보 처리 목적</td></tr>
<tr><td>고객의 소리</td><td>103,257</td><td colspan="2">[필수] 성명, 휴대전화번호, 이메일, 민원내용
[선택] 없음</td><td>해당없음</td><td>홈페이지 답변처리 및 게시글 조회, 수정, 삭제</td></tr>
</table>

개인정보 영향평가 요약본

개요	홈페이지 사용등록 교직원 정보	705,365	**[필수]** ID, 비밀번호, 성명, 생년월일, 휴대전화번호, 주소, 학교기관번호, 정보수신 동의(SMS,이메일,우편물 중 1이상), 성별, 내외국인 여부, 통신사, CI **[선택]** 이메일, 자택전화번호, (인증서 로그인 시)인증서	해당없음	홈페이지 사용등록 교직원 내역관리
	교직원 대여 정보	246,406	**[필수]** 주민등록번호, 대여금액, 대여종류, 증빙서류(가족관계증명서), 계좌번호 **[선택]** 없음	해당없음	교직원 생활자금 대여, 국고학자금 대여 내역 관리
	교직원 급여증서 정보	742,000	**[필수]** 성명, 집주소, 휴대전화번호, 이메일, 주민등록번호, 증서번호, 계좌번호 **[선택]** 없음	해당없음	교직원 급여 증서 관리
	교직원 월연금 정보	109,923	**[필수]** 증서번호, 연금개시일, 최종연금지급년월, 연금지급종료일, 총지급액, 총지급횟수, 월지급액 **[선택]** 없음	해당없음	연금 수급자 월연금 지급 내역 관리
	교직원 부담금 징수 정보	965,886	**[필수]** 교직원번호, 고지년월, 학교기관, 부담금종류, 고지금액, 수납여부 **[선택]** 없음	해당없음	교직원 부담금 고지 및 징수 내역 관리
	교직원 소득총액 정보	642,187	**[필수]** 교직원번호, 근무일수, 소득총액, 기준소득월액, 임용일 **[선택]** 없음	해당없음	교직원의 소득총액 신고 및 관리
	교직원 신분변동 정보	968,223	**[필수]** 교직원번호, 학교기관번호, 직위, 학력, 경력, 호봉, 정근, 승인월, 신분상태, 기준월액, 종전보수월액, 발령종류 **[선택]** 없음	해당없음	교직원의 신분변동 내역 관리
	교직원 재직기간 정보	969,541	**[필수]** 교직원번호, 종류, 총승인월수, 시작일, 종료일, 공백월, 납부총액, 최종고지월, 납부종료코드 **[선택]** 없음	해당없음	교직원의 재직기간(군소급, 소급통산 등) 관리
	교직원 합산 정보	83,715	**[필수]** 교직원번호, 재직기간, 직위, 호봉, 정근, 급여지급액, 분할횟수, 보수월액, 특례여부, 기준소득월액 **[선택]** 없음	해당없음	교직원의 합산내역 관리
	교직원 재해보상	14,011	**[필수]** 성명, 집주소, 휴대전화번호, 이메일, 주민등록번	해당없음	교직원 재해보상 내역

개인정보 영향평가 요약본

	정보		호, 문서번호, 보수월액, 상병명, 심의회번호, 교직원번호, 계좌번호, 폐질등급, 교직원번호, 가해자성명, 가해자주민번호, 가해자주소 **[선택]** 없음		관리
	교직원 급여지급 정보	797,000	**[필수]** 급여결정번호, 임용일, 퇴직일, 재직기간, 공백월, 지급일, 급여액, 교직원번호, 증서번호 **[선택]** 없음	해당없음	교직원 급여지급 내역 관리
	교직원 연금 기초 정보	1,045,045	**[필수]** 성명, 주민등록번호, 교직원번호, 소속학교기관, 임용일, 최종학력, 자격, 경력기간, 직위, 호봉, 정근, 표준보수월액, 부담금, 재직월수, 해당년월, 부담금액, 기준소득월액 **[선택]** 없음	해당없음	교직원의 직위, 자격 및 경력 등에 따라 보수월액 및 기준소득액 관리
	교직원 환수 정보	7,034	**[필수]** 환수번호, 환수결정일, 환수사유, 환수원금, 환수이자, 환수자명, 주소, 전화번호, 월반납금, 교직원번호 **[선택]** 없음	해당없음	교직원의 급여 환수내역 관리

개인정보 흐름분석

○ 수집

업무	수집정보	수집경로	수집대상	근거
홈페이지	- 회원관리 정보 - 고객의소리/민원 정보	온라인	- 연금가입자/수급자	- 정보주체 동의
복지서비스	- 회원가입/관리 정보 - 복지서비스관리 정보	온라인	- 연금가입자/사립학교공무직/제휴업체담당자 - 복지시스템회원	- 정보주체 동의
연금서비스	- 대여업무관리 정보 - 퇴직급여관리 정보 - 요양급여관리 정보 - 부조급여관리 정보 - 재직자기간관리 정보	온라인	- 연금가입자	- 정보주체의 동의 - 사학연금법/동법 시행령
부정수급예방서비스	- 신상조사대상자 식별정보/얼굴사진/생제정보 - 연금수급자 소득정보	오프라인, 온라인	- 신상조사대상자/연금수급자	- 정보주체의 동의 - 사학연금법/동법 시행령

○ 보유·이용

업무	보유·이용정보	보유	암호화	이용목적
홈페이지	- 회원관리 정보 - 고객의소리/민원 정보	DB	비밀번호	- 본인확인/연금가입 여부 확인 - 작성자 확인/결과통지
복지서비스	- 회원가입/관리 정보 - 복지서비스관리 정보	DB	비밀번호	- 본인확인/연금가입 여부 확인 - 신청자 확인/결과통지

개인정보 영향평가 요약본

업무	보유·이용정보	보유	암호화	이용목적
연금서비스	- 교직원/퇴직급여 정보 - 대여업무관리 정보 - 퇴직급여관리 정보 - 요양급여관리 정보 - 부조급여관리 정보 - 재직자기간관리 정보 - 연금수급자관리 정보 - 확인서발급처리 정보	DB	고유식별정보, 비밀번호, 계좌번호	- 이용자의 조회 요청 처리 - 신청접수/처리요건심사/부인방지 - 신청자정보조회/조회조건처리 - 신청자정보조회/확인서발급
부정수급예방서비스	- 신상조사대상자 식별정보/얼굴사진/생체정보 - 금융재산환수 정보 - 연금수급자 소득정보	DB, 연계이용	얼굴사진, 안면인식 특징정보, 고유식별정보	- 생체정보를 이용한 신상조사/신상조사 업무 관리 - 부정수급자 금융재산 환수 - 수급대상자 연금지급액 산정

○ 제공

- 대상시스템에서 처리하는 개인정보를 제3자에게 제공하는 경우는 없음

○ 위탁

- 공단은 19개의 개인정보 처리업무를 위탁하고 있으며, 공단 대표 홈페이지에 게시한 개인정보처리방침 4(개인정보처리 위탁)에서 개인정보 처리업무 위탁명, 계약기간, 수탁기관명을 정보주체에게 공개하고 있음
- 공단은 개인정보 처리업무 위탁 시 개인정보 관리에 관한 책임사항 등이 포함된 개인정보 처리 위탁계약서를 작성하였음.
- 대상시스템에서 처리하는 개인정보 처리업무를 위탁받아 처리하는 수탁업체를 대상으로 개인정보보호 교육, 처리현황 점검 등 관리 · 감독 활동을 이행하고 있음

○ 파기

- 홈패이지 회원관리 정보, 교직원/퇴직급여 정보 등 연금서비스 관련 정보 및 신상조사를 위한 얼굴정보/생체정보 등은 영구보관으로 파기하지 않음
- 홈페이지 고객의소리/민원 정보는 보유기간 5년으로 보유기간 만료 시 파기함
- 복지서비스를 위한 회원가입/관리 정보, 복지서비스관리 정보는 보유기간이 산정되지 않았거나 파기절차가 정해지지 않은 상태임

○ 개인정보 처리 흐름도

- [붙임] 개인정보 처리 흐름도 참조

영향평가 기준

평가기준 변경사항 및 사유

○ 106개 평가항목 기준

- 영향평가 안내서 85개 항목 + 추가 35개 항목 - 제외 14개 항목

○ 지표추가 항목

- 자동화된 결정, 가명정보 처리, 이용/제공내역 통지, 공공시스템 보호조치, 생체인식정보, 클라우드 보안 등 법령 개정사항 및 신기술 적용에 따른 보호조치 등 35개 항목 추가

○ 지표삭제 항목

- CCTV, RFID, 위치정보 등은 대상시스템과 관련없는 14개 항목 제외

○ 지표변경 항목

- 정보주체의 권리 중 전송·동의철회, 만 14세 미만자에 대한 법정대리인 동의 확인 등 14개 항목 일부 변경

개인정보 영향평가 요약본

주요 평가기준	○ 법령요구사항에 따른 항목 추가 및 변경 반영 - 23.9.22 시행 개인정보 보호법 제21조(개인정보의 파기) 제1항 - 23.9.22 시행 개인정보 보호법 제22조의2(아동의 개인정보 보호) 제1항 - 23.9.22 시행 개인정보 보호법 제38조(권리행사의 방법 및 절차) 제1항, 제4항 - 23.9.22 시행 개인정보의 안전성 확보 조치 기준 고시 제4조(내부 관리계획의 수립·시행 및 점검) 제3항 - 23.9.22 시행 개인정보의 안전성 확보 조치 기준 고시 제5조(접근 권한의 관리) 제3항 - 23.9.22 시행 개인정보의 안전성 확보 조치 기준 고시 제6조(접근통제) 제6항 - 23.9.22 시행 개인정보의 안전성 확보 조치 기준 고시 제7조(개인정보의 암호화) 제1항, 제2항, 제4항, 제5항 - 23.9.22 시행 개인정보의 안전성 확보조치 기준 고시 제14조~제17조 (공공시스템 운영기관 등의 개인정보 안전성 확보조치) ○ 발주기관에서 요청하는 대상시스템 관심사항 평가 반영 - 행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용 기준 및 안전성 확보 등에 관한 고시 제7조~제15조 - 주요정보통신기반시설 취약점 분석/평가 기준 내 클라우드 취약점 분석/평가 항목 - 생체정보 보호 가이드라인(2021. 9, 개인정보보호위원회)
평가기준에 따른 개인정보 침해요인 분석·평가	○ 대상시스템에서 개인정보 수집은 개인정보 보호법 제15조 정보주체의 동의 및 법률에 근거하여 적법하게 수집하고 있으며, 개인정보를 제3자에게 제공하지는 않음. - 개인정보보호법 제15조 제1항, 제3항 - 사학연금법 제18조, 제31조의2, 제32조, 제33조, 제33조의2, 제33조의3, 배34조 - 사학연금법 시행령 제47조의2, 제63조의2, 제63조의3, 제97조 ○ 개인정보 처리 및 기술적 보호조치 분석 결과 - 대상시스템은 홈페이지, 복지서비스, 연금서비스, 부정수급예방서비스 등의 업무처리 및 목적에 따라 14개의 개인정보파일을 운영하고 있으며, 개인정보법 제32조, 동법 시행령 제33조, 표준개인정보보호지침 제58조에 근거하여 적법하게 개인정보파일 대장 작성, 개인정보보호 종합지원시스템에 등록 및 홈페이지에 공개하고 있음. - 기술적 보호조치 분석 결과 접근통제, 악성프로그램 등 방지, 물리적 접근 방지, 개인정보의 파기 등 세부분야에서 안전성확보조치 개인정보의 안전성 확보 조치 기준 고시에 근거하여 적법하게 운영하고 있음. ○ 개인정보 침해 위험 요소 - 개인정보 수집/이용 시 동의 요건 미준수 등 수집 분야의 일부에 침해요소가 존재 (3.1.1, 3.1.5, 3.1.6) - 처리하는 개인정보파일 일부 보유기간 미산정, 파기 미결정 등 보유 및 파기 분야의 일부에 침해요소가 존재 (3.2.1, 3.5.1) - 관리자 로그인 시 안전한 인증수단(Multi-Factor 인증, 비밀번호 복잡도 규칙 등) 미적용 등 접근권한 관리 분야의 일부에 침해요소가 존재 (4.1.2, 4.1.3, 4.1.5, 4.1.7, 4.1.9) - 인증정보가 포함된 첨부서류를 암호화 하지 않는 등 개인정보의 암호화 분야 및 생체정보 활용 분야의 일부에 침해요소가 존재 (4.3.1, 4.3.4, 5,3,8) - 개인정보처리방침에 생체인식정보 처리 내용을 안내하고 있지 않는 등 생체정보 활용 분야의 일부에 침해요소가 존재 (5.3.10)

개인정보 영향평가 요약본

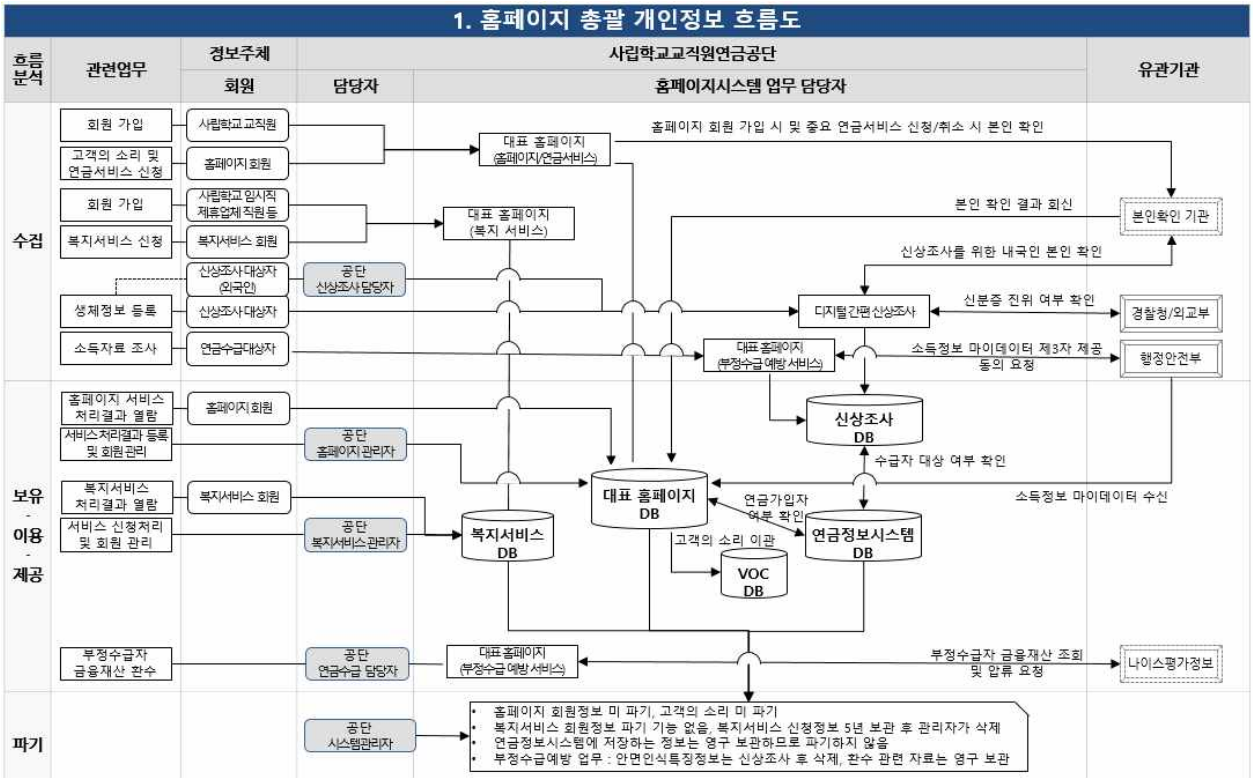
		- 클라우드컴퓨팅서비스 관리 포털 IAM 계정 접속 시 접속IP를 제한하도록 설정하지 않는 등 클라우드 보안 분야의 일부에 침해요소가 존재 (5.5.6, 5.5.7)
위험요인에 대한 개선조치	주요 위험요소에 따른 개선조치 방안	○ 개선계획 (2024년1월) 1. 로그인 인증기능 강화 (4.1.2) 2. 로그인 실패 허용횟수 초과 시 접속 제한조치 적용 (4.1.5) 3. 부정수급예방서비스 접속 세션 타임아웃 설정 (4.1.6) 4. 소스코드 내 암호키 노출 방지 조치 적용 (4.3.1, 5.3.8) 5. 인터넷을 통한 개인정보 송수신 시 안전한 암호화 프로토콜 적용 (4.3.4) 6. 부정수급예방서비스 개인정보 접속내역 기록 시 필수항목 추가 (4.4.1) 7. 개인정보보호 관련 정책 개정 (1.2.1) 8. 미성년자 개인정보 수집·이용 동의 절차 적용 (3.1.5) 9. 접근권한 관리 이력 보관기능 구현 (4.1.9) 10. 개인정보처리방침 내 생체인식정보 처리 내용 안내 (5.3.10) 11. 클라우드컴퓨팅서비스 자산 접근통제 강화 (5.5.6, 5.5.7) ○ 개선계획 (2024년3월) 12. 개인정보 수집·이용 동의서식 제·개정 (3.1.1, 3.1.6) 13. 중요 개인정보가 포함된 비 정형 전자문서 저장 시 암호화 적용 (4.3.1) 14. 개인정보 보유기간 책정 및 파기 기능 적용 (3.2.1, 3.5.1) 15. 중요 화면 접근 시 본인확인 절차 수립 (4.1.3) 16. 운영 데이터 이용 절차 개선 (4.8.1) ○ 개선계획 (2024년6월) 17. 시스템에 대한 비정상 접근방지 보호대책 적용 (4.1.7) 18. 개인정보 노출방지 기능 적용 (4.8.2) ○ 개선계획 (2024년9월) 19. 공공시스템 접속계정 관리절차 개선 (4.10.2) 20. 공공시스템 이용기관용 접속기록 점검 기능 구현 (4.10.3) 21. 공공시스템 개인정보 침해시도 발생 시 정보주체 통지절차 개선 (4.10.4)
	위험요소에 따른 정보주체 인지사항	○ 개인정보 수집·이용 동의서식 제·개정 필요 ○ 미성년자 개인정보 수집·이용 동의 절차 적용 필요 ○ 개인정보 보유기간 책정 및 파기 기능 적용 필요 ○ 중요 개인정보가 포함된 비 정형 전자문서 저장 시 암호화 적용 필요 ○ 개인정보처리방침 내 생체인식정보 처리 내용 안내 필요 ○ 공공시스템 개인정보 침해시도 발생 시 정보주체 통지절차 개선 필요
평가결과		○ 공단의 개인정보보호 관리체계 영역에 대한 점검 결과, 개인정보보호 조직 및 개인정보 보호 계획, 개인정보 침해대응, 정보주체 권리보장 등에 관한 규정·지침을 수립하는 등 양호하나, 최근 법령 개정사항이 규정·지침에 반영되지 않음

개인정보 영향평가 요약본

	○ 홈페이지시스템의 개인정보보호 관리체계 영역에 대한 점검 결과, 개인정보취급자 관리, 개인정보파일 관리, 개인정보처리방침에 관한 규정·지침이 적정히 수립되었고 이에 따라 체계적으로 관리되고 있으므로 양호함 ○ 개인정보처리 단계별 보호조치 영역에 대한 점검 결과, 이용·제공 시 보호조치와 개인정보 처리업무 위탁 시 보호조치는 양호하게 이행하고 있으나, 수집·이용에 대한 동의를 누락하거나 동의요건을 충족하지 못하는 경우가 있으며, 보유기간을 과다하게 책정하거나, 회원 탈퇴 시 파기절차가 수립되어 있지 않는 등 일부 취약사항이 발견되어 개선이 필요함 ○ 대상시스템의 기술적 보호조치 영역에 대한 점검 결과, 접근통제, 악성프로그램등 방지, 물리적 접근방지 등은 대체로 양호하게 운영되고 있으나, 취급자 인증방식이 안전하지 않거나, 로그인 실패 허용 횟수 제한 또는 세션 타임아웃을 적용하지 않거나, 중요 개인정보 변경 시 본인 여부를 확인하지 않거나, 주요 개인정보취급자에 대한 추가 인증방식을 적용하지 않고, 취급자에 대한 접근권한 이력을 기록·관리하지 않으며, 인터넷을 통한 개인정보 송수신시 안전하지 않은 암호화 프로토콜을 사용하는 등 일부 침해요인이 발견되어 개선이 필요함 ○ 특정 IT기술 활용 시 개인정보보호 영역에 대한 점검 결과, 생체인식정보 처리에 관한 사항을 개인정보처리방침에 안내하지 않거나, 클라우드 시스템 접속 시 IP 제한, 장기 미 사용자 접근제한 등 일부 침해요인이 발견되어 이에 대한 개선이 필요함

[붙임] 개인정보 처리 흐름도

1. 홈페이지 총괄 개인정보 흐름도



5. 부정수급예방서비스 총괄 개인정보 흐름도