

한국마사회 개인정보 영향평가

인사관리시스템 개인정보 영향평가서 요약본

2024. 4.



개인정보 영향평가서 요약본							
공공기관 명		한국마사회					
평가기관		(주)한국아이티컨설팅	평가기간	2024.03.13. ~ 2024.04.30.	평가예산	☐ 1천만원 미만 ☒ 1천만원 이상 ~ 3천만원 미만 ☐ 3천만원 이상 ~ 5천만원 미만 ☐ 5천만원 이상 ~ 1억원 미만 ☐ 1억원 이상	
평가대상시스템개요	시스템명		인사관리시스템(SAP ERP)			시스템 구축 또는 변경 일정	2023.06.30. ~ 2024.06.29.
	추진개요 및 목적		- S/4HANA의 빅데이터 분석 기술을 이용한 재무(수익, 비용), 인사, 노무(총액인건비 등), 예산 데이터 검증 및 수요예측으로 지능형 예측경영, RISK 관리 실현 기반 마련 - S/4HANA Cloud(RISE with SAP) 도입을 통해 안정적이고 효율적인 운영환경 확보 - SAP기능 고도화를 통한 비즈니스 처리절차 간소화로 업무 효율성 향상 및 신속한 경영정보 제공(재무결산 및 보고자료 작성시간 단축) - 고성능 인메모리 기반의 대용량 데이터 처리를 통한 속도 개선 - 클라우드 방식 인프라 도입을 통한 노후화된 정보자원 또는 정보시스템의 복잡도 제거로 운영관리 부담 최소화, 관리 효율성 증대, 정부정책 준수 기여				
	추진성격	대상여부	- 개인정보보호법 시행령 제35조 제1호 해당 - 5만 명 이상 민감정보·고유식별정보 처리			추진 예산	5,590,200천원
		추진주체	정보화사업부				
		추진근거	2023년 차세대 ERP시스템 전환 사업 추진계획			추진 유형	☐ 신규 구축 ☒ 변경(고도화) ☐ 운영
		신기술 유형	프라이빗 클라우드(Public Cloud) 컴퓨팅서비스 사용				
	주요내용		- SAP ERP 업그레이드와 인프라 아키텍처 재구성 - ECC6.0→S/4HANA Cloud(RISE with SAP Cloud, Private Cloud Edition) - 모듈별 마스터데이터 이관 및 검증 - S/4HANA 기반의 기존 프로그램 코드 최적화 작업 수행 - 자금/회계/조달/예산/인사 프로그램 재정의 및 S/4HANA의 스탠다드 기능으로 전환 및 부분 고도화 - 인사행정, 근태, 교육, 평가, 출장, 급여, 복리후생 관리 - 웹표준 기반의 ESS 시스템 구축 - 연계시스템 인터페이스 방식 통합 개발				
운용체계 변경내용 (변경인 경우)		해당 없음					
개인 정보 파일 개	파일명	정보주체 수	개인정보 항목		제3자 제공		개인정보 처리 목적
	직원정보	83,542건	필수: 성명, 생년월일, 집연락처, 집주소, 핸드폰, 이메일, 주민등록번호, 사번, 계좌번호, 병역사항, 학력사		- 제공근거: 장애인고용촉진 및 직업재활법 제27조 - 제공받는자: 한국장애인고용공단 - 제공목적: 장애인고용실태		근로계약의 체결·이행, 이해충돌방지

요			항, 경력사항, 가족사항, 자격사항, 장애사항, 보훈사항, 친인척 재직자 정보 선택: 없음	제출 • 제공항목: 성명, 주민등록번호, 장애인등록번호 • 제공근거: 보훈대상자 지원에 관한 법률 제40조 • 제공받는자: 보훈부 • 제공목적: 보훈대상자 신고 • 제공항목: 성명, 생년월일, 주소, 핸드폰, 보훈번호, 가족사항 • 제공근거: 국민연금법 제123조, 국민건강보험법 제96조, 고용보험법 제110조 • 제공받는자: 국민연금공단, 국민건강보험공단, 근로복지공단 • 제공목적: 보험가입 • 제공항목: 성명, 주민등록번호 • 제공근거: 국세기본법 제85조 • 제공받는자: 국세청 • 제공목적: 연말정산 • 제공항목: 성명, 주민등록번호, 집주소, 계좌번호	
개인정보 처리 흐름분석	• 개인정보 수집 단계 - 임직원의 개인정보는 「근로기준법」 제41조, 「소득세법」 제127조, 「보훈대상자 지원에 관한 법률」 제40조, 「장애인고용촉진 및 직업재활법」 시행령 제27조, 「국민연금법」 제123조, 「공직자의 이해충돌방지법」 제5조에 근거해 수집함 - 친인척 재직자 정보는 정보주체의 동의를 받아 수집함 • 개인정보 보유·이용, 제공, 위탁 단계 - 수집한 임직원 개인정보는 인사행정관리, 근태/교육/평가/출장관리, 급여/복지후생관리에 이용함 - 임직원 개인정보는 「국민연금법」 제123조, 「국민건강보험법」 제96조, 「고용보험법」 제110조, 「장애인고용촉진 및 직업재활법」 시행령 제27조, 「보훈대상자 지원에 관한 법률」 제40조, 「국세기본법」 제85조에 근거해 국민연금공단, 국민건강보험공단, 근로복지공단, 국세청은 해당 기관이 마련한 시스템에 접속하여 제공하고 한국장애인고용공단과 보훈부에는 공문으로 발송하여 제공함 - 대상시스템 구축을 위해 KPMG컨소시엄과 개인정보처리 위탁 계약을 체결, 개인정보처리 방침에 위탁 사실 공개, 수탁자 관리·감독을 하고 있으며 개인정보처리 재위탁은 하고 있지 않음 • 개인정보 파기 단계 - 공공기록물 관리에 관한 법률」 제19조에 따른 공공기관 공통업무 보존기간 준칙에 의거해 '준영구' 보관으로 책정하여 파기 대상 개인정보는 없음 • 개인정보 처리 흐름도 : [붙임] 참조				
영	평가기준	추가	• 대상기관 개인정보보호 관리체계 평가영역 (2개 평가항목)		

향 평 가 기 준	변경사항 및 사유		- 개인정보 침해대응 : 손해배상 보장 (사유: 개정 「개인정보보호법」(2024.3.15. 시행) 제39조의7 반영) - 정보주체 권리보장 : 개인정보 이용·제공내역 통지(1.4.3) (사유: 개정 「개인정보보호법」(2024.3.15. 시행) 제20조의2 반영) • 특정 IT기술 활용 시 개인정보보호 평가영역 (2개 평가항목) - 클라우드컴퓨팅 서비스 보호조치 : 클라우드컴퓨팅 서비스 보호조치 (사유: 대상시스템이 프라이빗 클라우드에서 운영됨에 따라 관련 항목 반영)
		변경	• 대상기관 개인정보보호 관리체계 평가영역 (3개 평가항목) - 개인정보보호 계획 : 내부관리계획 이행 점검 (사유: 개정 「개인정보의 안전성 확보조치 기준」 제2023-6호 제4조 반영) - 개인정보 침해대응 : 유출사고 대응(1.3.2) (사유: 개정 「개인정보보호법」(2024.3.15. 시행) 제34조 반영) - 정보주체 권리보장 : 정보주체 권리보장 절차 수립(1.4.1) (사유: 개정 「개인정보보호법」(2024.3.15. 시행) 제37, 20조 반영) • 개인정보 처리단계별 보호조치 평가영역 (5개 평가항목) - 수집 : 동의받는 방법의 적절성(3.1.5) (사유: 개정 「개인정보보호법」(2024.3.15. 시행) 제22조의2 반영) - 위탁 : 위탁사실 공개(3.4.1), 위탁계약(3.4.2), 수탁사 관리·감독 (3.4.3) (사유: 개정 「개인정보보호법」(2024.3.15. 시행) 제26조 반영) - 파기 : 파기계획 수립(3.5.1) (사유: 개정 「개인정보보호법」(2024.3.15. 시행) 제21조 반영) • 대상시스템의 기술적 보호조치 평가영역 (7개 평가항목) - 접근권한 관리 : 인증 관리(4.1.2, 4.1.5) (사유: 개정 「개인정보의 안전성 확보조치 기준」 제2023-6호 제5조 반영) - 개인정보의 암호화 : 저장 시 암호화(4.3.1), 전송 시 암호화(4.3.3) (사유: 개정 「개인정보의 안전성 확보조치 기준」 제2023-6호 제7조 반영) - 접속기록의 보관 및 점검 : 접속기록 보관(4.4.1), 접속기록 점검 (4.4.2), 접속기록 보관 및 백업(4.4.3) (사유: 개정 「개인정보의 안전성 확보조치 기준」 제2023-6호 제2, 8조 반영)
		삭제	• 대상시스템의 기술적 보호조치 평가영역 (1개 평가항목) - 2023.9.22. 시행 개인정보의 안전성 확보조치 기준에서 삭제됨에 따라 해당 지표(4.2.4) 삭제 • 특정 IT기술 활용 시 개인정보보호 평가영역 (16개 평가항목) - 대상시스템에서 CCTV, RFID, 생체인식정보, 위치정보 등 특정 IT 기술을 활용하지 않아 16개 지표(5.1.1 ~ 5.4.2) 삭제
	주요 평가기준		• 입퇴사가 빈번한 특정 직군과 준연구 보관 기준을 가진 한국마사회의 특성을 감안하여 퇴직자 정보 분리보관(3.5.2)을 중점 평가함 • 입사 시 수집하는 개인정보를 최소화·현행화하기 위해 개인정보 수집의 적합성 분야(3.1.1, 3.1.2)를 중점 평가함 • 접속기록을 접속기록 관리솔루션으로 관리하고 있지 않아 접속기록의 보관 및 점검 분야(4.4.1~4.4.3)를 중점 평가함
평가기준에 따른 개인정보 침해요인 분석·평가			• 영향평가 결과 “이행(양호)”로 평가된 사항 ① 개인정보보호법 등 관련 법령 준수 여부에 대한 분석·평가 - 「근로기준법」 제41조, 「소득세법」 제127조, 「보훈대상자 지원에 관한 법률」 제40조, 「장애인고용촉진 및 직업재활법」 시행령 제27조, 「국민연금법」 제123조, 「공직자의 이해충돌방지법」 제5조에 근거하여 적법하게 수집하고 있으며, 친인척 재직자 정보는 정보주체의 동의를 받아 수집하고 있음. - 임직원의 개인정보는 「국민연금법」 제123조, 「국민건강보험법」 제96조, 「고용보험법」 제110조, 「장애인고용촉진 및 직업재활법」 시행령 제27조, 「보훈대상자 지원에 관한 법

		를」 제40조, 「국세기본법」 제85조에 근거하여 적법하게 국민연금공단, 국민건강보험공단, 근로복지공단, 한국장애인공단, 보훈부, 국세청에 제공하고 있음 ② 개인정보 처리, 개인정보처리시스템 운영관리 및 기술적 조치 사항에 대한 분석·평가 - 대상시스템에서 수집·제공하는 개인정보는 그 목적에 필요한 최소한의 범위로 운영하고 있음 • 영향평가 결과 “부분이행” 또는 “미이행”으로 평가된 사항 (비공개)
위험요인에 대한 개선조치	주요 위험요소에 따른 개선조치 방안	(비공개)
	위험요소에 따른 정보주체 인지사항	• 대상 시스템은 정보주체(임직원)가 접속·이용할 수 없는 시스템으로 “부분이행” 또는 “미이행”으로 평가된 사항 중 정보주체가 알아야 할 위험요소 및 위험요소를 제거하기 위해 노력해야 할 사항은 없음
평가결과		• 인사관리시스템의 개인정보처리에 따른 침해 위험성을 아래 평가영역 별로 분석·평가하였음 - 대상기관의 개인정보보호 관리체계 (11개 평가항목) - 대상시스템의 개인정보보호 관리체계 (6개 평가항목) - 개인정보 처리단계별 보호조치 (21개 평가항목) - 대상시스템의 기술적 보호조치 (32개 평가항목) - 특정 IT기술 활용 시 개인정보보호 (2개 평가항목) • 총 72개의 지표 평가 결과 ‘이행’ 63개, ‘부분이행’ 3개, ‘미이행’ 3개, ‘해당없음’ 3개 항목이 식별되어 6건의 개선과제가 도출되었으며, 전체 이행률은 93%로 평가되었음 • 대상기관의 개인정보보호 관리체계 평가 영역에서 개인정보 보호조직, 개인정보 보호계획, 개인정보 침해대응, 정보주체 권리보장 등 총 4개 평가분야, 11개 평가항목이 모두 이행되어 이행률은 100%로 평가되었음 • 대상시스템의 개인정보보호 관리체계 평가 영역에서 개인정보취급자 관리, 개인정보파일 관리, 개인정보처리방침 분야 등 총 3개 평가분야, 6개 평가항목이 모두 이행되어 이행률은 100%로 평가되었음

- 개인정보 처리단계별 보호조치 평가 영역에서 개인정보 수집, 보유, 이용·제공, 위탁, 파기 분야 등 총 5개 분야의 21개 항목 중 19개 항목이 '이행', 1개 항목(평가항목 : 3.5.2)이 '미이행', 1개 항목이 '해당 없음'으로 식별되어 이행률은 95%로 평가되었음 (비공개)

[붙임] 개인정보 처리 흐름도

