개인정보 영향평가서 요약본

<table>
<tr><td colspan="2">공공기관 명</td><td colspan="5">한국해양교통안전공단</td></tr>
<tr><td colspan="2">평가기관</td><td>㈜한국전산감리원</td><td>평가
기간</td><td>2025.07.07
~
2025.09.19</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">평가대상시스템 개요</td><td>시스템명</td><td colspan="3">KOMPAS</td><td>시스템
구축 또는
변경 일정</td><td>2019.11 ~ 2023.05</td></tr>
<tr><td>추진개요
및 목적</td><td colspan="5">○ 공단 내 주요 업무시스템 구축 후('07, '10, 고도화), 업무의 효율적 운용을 위한 정보시스템 개선 필요
○ 정부 대행업무의 체계적이고 원활한 수행을 위한 개선 추진
○ 공단 정보화 업무의 원활한 수행을 위한 표준 업무체계 수립 필요
○ 검사.연구개발 등 주요업무 전반을 지원하기 위한 관리시스템 구축 필요
○ Paperless 기반의 문서관리시스템 구축 필요
○ 정보화 인프라의 클라우드 전환을 위한 인프라 구축 필요
○ 공단 대내외 사용자 간 커뮤니케이션 및 연계를 위한 채널 구축 필요
○ 정보시스템 구축을 위한 데이터 모델 수립, 업무프로세스 정비 필요</td></tr>
<tr><td rowspan="4">추진성격</td><td>대상여부</td><td colspan="2">영향평가 대상 아님</td><td rowspan="2">추진예산</td><td rowspan="2">4,200,000천원
(VAT 포함)</td></tr>
<tr><td>추진주체</td><td colspan="2">한국해양교통안전공단</td></tr>
<tr><td>추진근거</td><td colspan="2">KOMPAS 구축 사업 계획</td><td>추진유형</td><td>□ 신규 구축
□ 변경(고도화)
■ 운영</td></tr>
<tr><td>신기술
유형</td><td colspan="4">해당사항 없음</td></tr>
<tr><td>주요내용</td><td colspan="5">○ 업무 및 정보화 표준 프로세스 정립
○ 통합 업무정보시스템 구축
○ 효율적인 추진체계 구성/운영
○ 클라우드 기반 정보화 인프라 구축</td></tr>
<tr><td>운용체계
변경내용
(변경인
경우)</td><td colspan="5">○ 해당없음</td></tr>
</table>

개인정보파일개요	파일명	정보주체 수	개인정보 항목	제3자 제공	개인정보 처리 목적
	KOMPAS 회원정보 (가칭)	1,445건	**[필수항목]** 아이디, 비밀번호, 성명, 휴대폰번호, 전자우편 **[선택항목]** 전화번호, 팩스번호, 주소, 회사명, 부서	-	KOMPAS 회원관리
	선박검사 정보파일	24,475건	**[필수항목]** 이름, 집연락처, 집주소, 핸드폰(연락처) **[선택항목]** E-Mail, 주민등록번호	-	선박검사관리
	안전운항 정보 (가칭)	771건	**[필수항목]** 성명, 상호, 선박명, 선박번호 **[선택항목]** 선장명, 선장 생년월일, 면허종류, 주소	-	여객선 안전 운항관리
	직원교육 이수내역 (가칭)	1,083건	**[필수항목]** 사원번호, 성명, 부서, 이메일, 직급, 교육이수내역, 보유스킬내역 **[선택항목]** -	-	직원 교육이수 내역 및 보유스킬 관리
	감사인정보 (가칭)	5건	**[필수항목]** 성명, 소속, 직급 **[선택항목]** 직종, 경력, 자격증, 교육실적	-	자체감사 감사인 관리
	외부감사 인정보 (가칭)	0건	**[필수항목]** 성명, 부서, 직위 **[선택항목]** 직급, 직책, 연락처, 이메일	-	외부감사 감사인 관리
	감사위원회 명부 (가칭)	0건	**[필수항목]** 성명, 생년월일, 휴대폰번호, 이메일, 주소, 위원회명, 임기기간	-	감사위원회 명부관리

			[선택항목] 직위, 학력, 경력		
	직원감사 정보 (가칭)	1,343건	**[필수항목]** 사번, 성명, 부서, 직책, 직위, 직급, 감사결과, 조치결과, 청렴교육수강이력 **[선택항목]** -	-	직원 감사결과 및 이행결과 관리
	외부강의 신고내역 (가칭)	313건	**[필수항목]** 성명, 부서, 직위, 직급, 요청인(기관명, 대표자명, 담당부서, 담당자, 연락처), 외부강의 내역 **[선택항목]** -	-	직원의 외부강의 신고 내역 관리
개인정보 처리 흐름분석		1. 개인정보 처리 내용 1) 회원관리 - 회원은 e-KOMSA 대외 포털에서 회원가입을 수행하며, 회원가입 시 SMS인증을 통해 본인임을 확인함 - 관리자는 회원의 가입내역을 확인 후 승인 처리함 - 회원은 e-KOMSA 대외 포털에서 로그인을 수행하며, 아이디/비밀번호를 알지 못할 시 아이디 찾기/비밀번호 찾기 기능을 통해 아이디 확인 및 비밀번호를 변경함 - 관리자는 회원정보를 조회, 수정, 삭제 등 회원정보를 관리함 2) 선박검사관리 - 선박 소유자/신청자는 한국해양교통안전공단 지사에 선박검사신청서 등 관련 자료를 준비한 후 선박검사 신청을 하며, 선박검사 업무담당자는 선박검사 신청 서류를 확인 후 선박검사 신청 접수 및 결재를 진행함 - 선박검사 업무담당자는 선박검사를 실시 후 검사보고서를 작성하며, 전표처리를 수행 함 - 선박검사 업무담당자는 신청서 처리, 선박검사 통계, 건명서 조회 등 선박검사 업무를 처리함 - 시스템은 해수부 MTIS 및 해수부 어선거래시스템과 내부연계를 하며, 해수부 수산정보통합시스템, 지콤스, 코디스 및 포트미스와는 연계시스템(ESB)을 통해 외부연계 함 3) 도면승인관리 - 도면승인 신청자는 온라인(e-KOMSA) 또는 한국해양교통안전공단 지사에 도면승인 신청서 등 관련 자료를 준비한 후 도면승인 신청을 하며, 도면승인 업무담당자는 도면승인 신청 서류를 확인 후 도면승인 신청 접수 및 결재를 진행함 - 도면승인 업무담당자는 도면승인 검사를 실시 후 검사보고서를 작성하며, 전표처리를 수행 함			

		- 도면승인 업무담당자는 중부지사에서 검사가 필요할 시 중부지사로 검사를 이첩하며, 중부지사 도면승인 업무담당자는 도면심사 배부 및 도면심사를 실시함 - 도면승인 신청자는 도면승인 신청 현황을 온라인(e-KOMSA)에서 조회 함 - 시스템은 해수부 MTIS 및 해수부 어선거래시스템과 내부연계를 하며, 해수부 수산정보통합시스템, 지콤스, 코디스 및 포트미스와는 연계시스템(ESB)을 통해 외부연계 함 4) 해양사고관리 - 해양사고담당자는 선박기본정보를 조회 후 해양사고정보를 입력함 5) 운항관리 - 공단의 운항관리 업무담당자는 여객선의 운항정보를 관리하기 위해 KOMPAS시스템에서 여객선정보를 등록함 - 해양경찰청 등 대상 기관은 대외포털(e-KOMSA)를 통해 여객선정보를 조회 및 출력함 6) LMS(교육관리) - 공단의 교육 업무담당자는 교육과정을 개설하며, 교육대상자를 선별함 - 교육대상자는 교육과정을 조회 후 교육을 신청함 - 공단의 교육 업무담당자는 교육신청 접수하며, 교육실시 결과를 관리하며, 교육대상자는 교육현황을 조회함 - 공단의 교육 업무담당자는 검사원 SKILL내역을조회하며, 검사원SKILL을 관리함 - 교육대상자는 전문SKILL취득현황을 조회하며, 공단의 교육 업무담당자는 교육생별/강사별 교육현황을 관리함 7) E감사 - 공단의 감사 업무담당자는 연별 감사계획을 수립함 - 공단의 감사 업무담당자는 감사계획에 의거 감사를 수행하며, 수감부서에 사전요청자료, 자료, 징구서등을 요구함 - 수감부서는 감사 업무담당자가 요청한 자료, 징구서 등을 제출함 - 공단의 감사 업무담당자는 감사결과를 등록하며, 감사대상자에게 처분, 소명 등을 요구함 - 감사 대상자는 처분 요구 조치 결과를 제출하며, 소명을 등록함 - 감사 대상자는 청렴교육을 등록하며, 외부강의 내역을 신고함 2. 개인정보 처리 흐름도 - [붙임] '개인정보 처리 흐름도' 참조
영향평가기준	**평가기준 변경사항 및 사유**	○ 특정 IT 기술 활용 시 개인정보보호(5장) : 6개 평가분야(고정형 영상정보 처리기기, RFID, 생체인식정보, 위치정보, 가명정보, 이동형 영상정보 처리기기) 30개 항목은 평가대상과 해당사항이 없어 평가에서 제외함.
	주요 평가기준	○『개인정보 영향평가에 관한 고시(2024.04.03.)』에 따른『개인정보 영향평가 수행 안내서(2024.04)』를 기준으로 평가를 실시함.
평가기준에 따른 개인정보 침해요인 분석·평가		1. 영향평가 수행 시 "이행" 으로 평가된 사항에 대하여 크게 2가지 사항 작성 1). 개인정보 보호법 등 관련 법령 준수 여부에 대한 분석평가 - 공단의 내부 관리계획에 개인정보 보호책임자 공식적 지정 - 공단의 개인정보 보호책임자는 개인정보 처리에 관한 업무를 담당하는 부서장

	으로 법적 요건을 충족하는 자로 지정 - 개인정보 보호책임자에게 법률 등에서 정하는 역할을 내부 관리계획에 공식적으로 부여 및 업무 수행 - 내부 관리계획을 수립하고 내부 의사결정 절차를 통해 공식적으로 시행 및 이행 실태를 연 1회 이상 점검 - 개인정보 침해사고(정보주체 권리침해, 개인정보 유출 등)에 대한 대응절차 마련 및 공식적으로 시행 - 정보주체의 개인정보 열람, 정정·삭제, 처리정지, 동의 철회 등 요구에 대하여 대응할 수 있는 처리 절차를 수립 및 공식적으로 시행 - 업무상 개인정보 취급 범위를 최소한으로 제한하고 업무수행에 필요한 최소한의 인원이 개인정보를 처리하도록 개인정보취급자 지정 - 개인정보취급자를 대상으로 역할 및 책임 부여 - "개인정보 처리방침"이라는 명칭을 사용하며, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분 안내 2). 개인정보 처리, 개인정보처리시스템 운영관리 및 기술적 조치사항에 따른 분석평가 - 정보주체 동의 및 법령에 근거한 개인정보 수집 - 정보주체 동의 시 4개 필수 사항 모두 안내 - 주민등록번호 수집 법정주의에 따라 법적 근거에 의해 수집 - 인터넷 홈페이지를 통하여 회원으로 가입 시 주민등록번호 대체 수단 적용 - 정보주체 동의 시 필수항목과 선택항목 구분 - 개인정보 동의 시 보유기간 등 중요한 내용을 명확히 표시 - 법령에 근거한 목적 외 이용·제공, 홈페이지 공개, 대장 작성 - 개인정보 처리에 관한 업무 위탁 시 개인정보처리방침에 공개, 개인정보처리 위탁 계약, 수탁자 관리·감독 실시 - 시스템 사용자 개별 계정 부여 - 접근통제시스템 설치·운영 - 외부에서 접근 시 VPN 방식의 접속 수단 적용 - 인터넷 홈페이지, P2P, 공유설정 등을 통한 개인정보 유·노출 보호조치 적용 - 웹 취약점 점검 등의 개발 보안 조치 적용 - 업무용 모바일 기기에 비밀번호 설정 등의 보호조치 적용 - 중요 정보를 DB에 저장 시 안전한 암호화 알고리즘 적용 - 업무용PC에 백신 프로그램 설치, 최신 업데이트 및 주기적 점검 - 전산실 출입통제 절차, 출입통제 대장 등 마련 - 전산실에 화재감지기 및 소화장비, UPS, 비상발전기, 항온항습기, 온습도센서 등의 보호설비 설치 및 운영 2. 영향평가 수행 시 "부분이행", "미이행"으로 평가된 사항에 대하여 개인정보 침해에 따른 위험요소 사항 - 개인정보 유출 상황을 대비한 모의훈련을 실시하지 않아 개인정보 유출 시 대응조직 구성, 대응방법, 유출 통지 및 신고 등이 체계적으로 대응하기가 어려울 수 있음 - 개인정보파일대장을 작성하지 않거나 적절히 관리하지 않아, 개인정보 처리에

	대한 법적 요구사항을 준수하지 못하거나 개인정보 안전성 확보조치를 준수하지 못하게 될 위험이 있음 - 개인정보파일을 변경하지 않거나, 보유하였음에도 신규 등록하지 않아 개인정보 보호위원회에 등록해야 하는 법적 요구사항을 준수하지 못하게 될 위험이 있음 - 개인정보처리방침을 작성할 때는 법령 등에 따른 모든 항목을 포함하여 작성 및 안내 하여야 하나, 개인정보처리방침에 안내된 내용이 현행화 되지않아 정보주체에게 개인정보 처리에 대해 명확하게 안내되지 않을 수 있음 - 개인정보 수집·이용 동의 여부를 KOMPAS에 기록하고 있지 않아 향후 개인정보 수집·이용 동의 여부를 확인할 수 없음 - 업무 목적에 필요한 최소한의 범위에서 개인정보를 수집하지 않아 개인정보 최소 수집 원칙을 준수하지 않을 수 있음 - 정보주체의 동의 없이 처리할 수 있는 개인정보의 항목과 그 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개하지 않아 정보주체의 알 권리를 침해 할 수 있음 - 개인정보 보유기간을 기관 내부의 공식적인 절차를 통해 산정을 하지 않고 개인정보를 보유함으로 인해 목적이 달성된 개인정보를 보유하게 되며, 이로 인해 개인정보의 무단 이용/제공, 노출 및 유출 위험이 증가할 수 있음 - 개인정보가 보유목적을 달성한 후에도 파기되지 않게 되어 개인정보 무단 이용·제공, 노출 및 유출 위험이 증가함 - 비밀번호를 정기적으로 변경하지 않고 초기(임시) 비밀번호를 즉시 변경하도록 하고 있지 않아, 악의를 가진 제3자가 비밀번호를 유추하여 알아내기가 용이하여 개인정보가 유출되거나 악의적인 용도로 도용될 위험이 있음 - KOMPAS에 대한 접근권한 부여, 변경 및 말소한 내역을 기록하지 않아 향후에 문제 발생 시 권한 발급 이력을 정확하게 파악하기가 어려워 책임추적성을 확보할 수없음 - 소스코드에 대한 취약점 점검을 실시하고 있지 않아 취약점으로 인해 개인정보가 유출, 노출될 위험이 있음 - 비밀번호를 해시함수를 통하여 단순히 일방향 암호화만 하는 경우에는 동일한 비밀번호를 사용하는 사용자는 동일한 해시값을 가지게 되며, 레인보우 테이블을 이용하면 해시값으로부터 비밀번호를 쉽게 추출해낼 수 있는 위험이 존재함. 또한 중요정보를 포함하고 있는 파일을 서버에 저장 시 암호화하고 있지 않아 개인정보 유출, 노출 등의 위험이 있음 - 암호화된 정보의 안전성을 확보하기 위해 암호키에 대한 보안과 제한된 관리자만 허용하도록 절차 수립 및 관리가 되어야 하나, 암호키에 대한 철저한 관리가 되지 않아 개인정보를 안전하게 보관하지 못하는 위험이 발생할 수 있음 - 개인정보를 정보통신망을 통해 인터넷 망 구간으로 송・수신하는 경우 암호화하지 않아 정보통신망을 통해 개인정보 유출, 노출 등의 위험이 있음 - 개인정보 등록, 수정, 삭제, 출력 등에 대한 접속기록을 보관하지 않아 개인정보 취급자의 불법적인 접근 및 행동을 확인하기가 어려울 수 있음 - 업무시간 외 개인정보 처리, 대량의 개인정보 조회 및 다운로드 등의 비정상 행위를 정기적인 점검을 통해 탐지 및 대응조치를 하지 않아 개인정보의 유출·변조·훼손 등에 대응하기가 어려울 수 있음 - 개인정보가 포함된 종이 인쇄물을 통해 개인정보가 유출되는 경우 인쇄물의 책임관계 및 출처 등이 명확하지 않아 책임추적성 확보가 어려울 수 있음

		- 개인정보의 출력(인쇄, 화면표시, 파일생성 등)시 용도에 따라 출력항목을 최소화하여 출력하고 있지 않아 개인정보의 유노출 위험이 있음 - 시스템 보호를 위한 재해·재난 대비 위기대응 매뉴얼 등 위기 대응 절차를 정기적으로 점검하고 있지 않으며 재해복구센터(DR센터)를 마련하지 않아 재해·재난 발생 시 체계적으로 대응할 수 없어 개인정보-의 손실 및 훼손 등이 발생할 수 있음
위험요인에대한개선조치	**주요 위험요소에 따른 개선조치 방안**	1. 평가기준에 따른 개인정보 침해요인 분석평가에서 작성된 "부분이행", "미이행"에 해당하는 사항 중 개인정보 처리, 대상시스템(개인정보처리시스템) 운영관리 및 기술적 조치사항에 대한 개선조치 방안 - 개인정보파일 관리 강화 - 개인정보처리방침 작성 강화 - 개인정보 수집·이용 동의 여부 기록 - 개인정보 최소 수집 - 개인정보 보유기간 최소한 산정 - 개인정보 지체없이 파기 - 비밀번호 관리 강화 - 접근권한 내역 기록 강화 - 개인정보 암호화 강화 - 개인정보 접속내역 기록·점검 강화 - 출력물 보안 강화 - 개인정보의 출력(인쇄, 화면표시, 파일생성 등) 시 출력항목 최소화 - 재해·재난 대비 위기대응 강화
	위험요소에 따른 정보주체 인지사항	○ 개인정보파일을 개인정보보호위원회에 등록 확인 ○ 개인정보 처리 현황을 개인정보 처리방침에 알기 쉽게 안내 확인 ○ 개인정보의 보유기간 및 파기 확인 ○ 비밀번호 주기적 변경 실시
평가결과		○ 대상기관 개인정보보호 관리체계(1장)는 10개 평가항목 중 9개의 항목을 이행(90%), 1개 항목을 부분이행(10%) 하고 있음. ○ 대상시스템 개인정보보호 관리체계(2장)는 6개 평가항목 중 3개의 항목을 이행(50%), 3개 항목을 부분이행(50%) 하고 있음. ○ 개인정보 처리단계별 보호조치(3장)는 25개 평가항목 중 해당없음으로 평가된 8개 항목을 제외하고 12개의 항목을 이행(48%), 4개 항목을 부분이행(16%), 1개 항목에 대해 미이행(4%) 하고 있음. ○ 대상시스템의 기술적 보호조치(4장)는 36개 평가항목 중 21개의 항목을 이행(58%), 11개 항목을 부분이행(31%), 4개 항목에 대해 미이행(11%) 하고 있음.

[붙임] 개인정보 처리 흐름도

1. 총괄 개인정보 흐름도

