인천공항출입국·외국인청
개인정보 영향평가 결과요약
<바이오정보전문분석시스템(BASE) 고도화 구축 사업>

2024. 12

KISCA (주)한국정보기술단
KOREA INFORMATION SYSTEMS CONSULTING & AUDIT Co.,Ltd

요 약

대상 시스템에 대한 개인정보 영향평가를 수행한 결과는 다음과 같음

- ○ 대상기관의 개인정보보호 관리체계 영역의 개인정보 침해 위험성을 평가한 결과, 4개 평가분야, 10개 항목 중 4개 항목에서 위험이 식별되었으며 개선계획을 수립함
- ○ 대상시스템 개인정보보호 관리체계 영역의 개인정보 침해 위험성을 분석·평가한 결과, 3개 분야 6개 항목에서 위험이 식별되지 않음
- ○ 개인정보 처리단계별 보호조치 영역의 개인정보 침해 위험성을 평가한 결과, 5개 평가분야, 26개 항목에서 위험이 식별되지 않음
- ○ 대상시스템의 기술적 보호조치 영역의 개인정보 침해 위험성을 평가한 결과, 9개 평가분야, 37개 항목 중 1개 항목에서 위험이 식별되었으며 개선계획을 수립함
- ○ 특정IT 기술 활용 시 개인정보보호 영역의 개인정보 침해 위험성을 평가한 결과, 9개 평가분야, 37개 항목 중 1개 항목에서 위험이 식별되었으며 개선계획을 수립함

가. 개인정보 보호조치 이행 현황

<개인정보 보호조치 이행 현황>

평가영역	평가분야	항목수	이행	부분 이행	미이행	해당 없음	이행율 (%)
1. 대상기관의 개인정보보호 관리체계	1.1 개인정보보호조치	2	0	2	0	0	50%
	1.2 개인정보보호 계획	3	1	1	1	0	50%
	1.3 개인정보 침해대응	2	2	0	0	0	100%
	1.4 정보주체 권리보장	3	2	0	0	1	100%
	소 계	**10**	**5**	**3**	**1**	**1**	**72.2%**
2. 대상시스템의 개인정보보호 관리체계	2.1 개인정보취급자 관리	2	2	0	0	0	100%
	2.2 개인정보파일 관리	2	1	0	0	1	100%
	2.3 개인정보처리방침	2	2	0	0	0	100%
	소 계	**6**	**5**	**0**	**0**	**1**	**100.0%**
3. 개인정보 처리단계별 보호조치	3.1 수집	10	3	0	0	7	100%
	3.2 보유	1	1	0	0	0	100%
	3.3 이용·제공	8	0	0	0	8	-
	3.4 위탁	4	4	0	0	0	100%
	3.5 파기	3	2	0	0	1	100%
	소 계	**26**	**10**	**0**	**0**	**16**	**100.0%**

평가영역	평가분야	항목수	이행	부분이행	미이행	해당없음	이행율(%)
4. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	10	1	0	0	9	100%
	4.2 접근통제	7	5	0	0	2	100%
	4.3 개인정보의 암호화	4	3	0	0	1	100%
	4.4 접속기록의 보관 및 점검	4	4	0	0	0	100%
	4.5 악성프로그램 등 방지	2	2	0	0	0	100%
	4.6 물리적 접근방지	2	2	0	0	0	100%
	4.7 개인정보의 파기	1	1	0	0	0	100%
	4.8 기타 기술적 보호조치	4	3	0	1	0	75.0%
	4.9 개인정보처리구역보호	3	3	0	0	0	100%
	소 계	**37**	**24**	**0**	**1**	**12**	**96.0%**
5. 특정IT 기술 활용 시 개인정보보호	5.3 생체인식정보	2	0	0	1	1	50%
	소 계	**2**	**0**	**0**	**1**	**1**	**50.0%**
합 계		**81**	**44**	**3**	**3**	**31**	**91.0%**

※ 이행율 = (이행 + 부분이행 * 0.5) / (이행 + 부분이행 + 미이행) * 100

나. 침해요인 분석

1) 대상기관의 개인정보보호 관리체계 침해요인

구분	부분이행	질의코드	1.1.1	준거성여부	의무
질의문	● 개인정보 보호책임자를 법령기준에 따라 지정하고 있습니까?				

평가근거 및 의견

<평가>

● 법무부 인천공항출입국·외국인청은 '개인정보보호 내부관리계획 Ⅱ. 개인정보보호 관리체계 2. 개인정보 보호책임자 지정'에서 개인정보 보호책임자를 총무과장으로 하도록 규정하고 있음

● 개인정보보호 경력의 법적기준 요건(개인정보 보호 경력 및 기술 경력 등)에 충족하는 개인정보 보호책임자 지정 필요하며, 인사발령 및 업무분장표 등을 통하여 개인정보보호 전담 조직 및 개인정보보호 책임자 지정이 되도록 개선이 필요함.

● 아울러, 대표홈페이지 개인정보처리방침 등에 법무부 인천공항출입국·외국인청의 개인정보 보호책임자 공개가 필요함.

● 개인정보 보호책임자(CPO) 지정 및 개인정보 보호조직 현황

구분	내용	점검결과
개인정보 보호조직 구성 및 운영 여부	개인정보보호 내부관리계획 Ⅱ. 개인정보보호 관리체계 1. 개인정보 보호 조직의 구성에 따라 조직 구성 및 운영	○
법적 기준을 충족하는지 여부	총무과장을 개인정보 보호책임자로 지정하고 있으나, 법적기준(개인정보 보호 경력 및 기술 경력 등)에는 충족하지 않음	△
인사발령 등을 통한 공식적 지정여부	개인정보보호 내부관리계획 Ⅱ. 개인정보보호 관리체계 1. 개인정보 보호 조직의 구성에 총무과장으로 공식적으로 지정	○
개인정보 보호책임자 지정 공개여부	개인정보처리방침 및 홈페이지를 통해 공개 되어 있지 않음	△

※ 점검결과 범례 : ○ : 적정, △ : 보완필요, × : 부적정

<의견>

● 법에서 요구하는 경력인정 요건에 맞는 개인정보 보호책임자 지정이 되어야 함 (개인정보 보호법 시행령 제32조 (개인정보 보호책임자의 자격) 제4항에 따라 개인정보 보호책임자로 지정되는 사람은 개인정보보호 경력, 정보보호 경력, 정보기술 경력을 합하여 총 4년 이상 보유하고, 그 중 개인정보보호 경력을 최소 2년 이상 보유해야 함)

● 개인정보처리방침 및 홈페이지 등을 통하여 개인정보보호 책임자가 공개되어야 함.

● 개인정보보호법 시행령 별표 1. 개인정보보호책임자 경력인정 요건

<정력인정 요건>

구분	정력 인정 요건	인정 기간
개인정보보호정력	○ 개인정보보호 관련 박사학위 취득자	3년
	○ 개인정보보호 관련 석사학위 취득자 ○ 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제14조에 따른 정보보호 및 개인정보보호 관리체계 인증심사원 ○ 개인정보 영향평가에 관한 고시 제5조에 따른 개인정보 영향평가 전문인력	2년
	○ 개인정보보호 관련 학사학위 취득자	1년
정보보호, 정보기술 정력	○ 정보보호, 정보기술 관련 박사학위 취득자	2년
	○ 정보보호, 정보기술 관련 석사학위 취득자	1년
	○ 정보보호, 정보기술 관련 학사학위 취득자	6개월

침해요인

- 개인정보 보호책임자는 개인정보 처리에 관한 전반적인 사항을 결정하고 이로 인한 제반 결과에 대해 책임을 지는 자임
- 개인정보 수집·이용·제공 등에 대하여 실질적인 권한을 가지고 있어야 하며 조직 내에서 어느 정도 독자적인 의사결정을 할 수 있는 지위에 있는 자여야 함
- 법률에서 요구하는 개인정보보호 책임자를 지정하지 않음으로 기관에서 개인정보 처리에 관한 업무를 실제적으로 책임질 수 없으며, 법에서 요구하는 사항에 위배될 수 있음

구분	부분이행	질의코드	1.1.2	준거성여부	의무
질의문	● 개인정보 보호책임자에게 법령 등에서 정하는 역할 및 책임에 관한 사항 정책화하고, 이에 근거해 관련 업무를 수행하도록 하고 있습니까?				
평가근거 및 의견	**<평가>** ● **[법률이 정하는 책임 역할 부여]** 법무부 인천공항출입국·외국인청은 '개인정보보호 내부관리계획 Ⅱ. 개인정보보호 관리체계 2. 개인정보 보호책임자 지정'에서 개인정보 보호책임자에 대하여 법률이 정하는 책임과 역할을 부여하고 있음 ● 개인정보 보호책임자의 업무부여 현황				

법률이 정하는 책임 및 역할	점검 결과	비고
개인정보보호계획의 수립 및 시행	○	
개인정보 처리실태 및 관행의 정기적인 조사 및 개선	○	
개인정보처리와 관련한 불만의 처리 및 피해구제	○	
개인정보 유출 및 오남용 방지를 위한 내부통제시스템의 구축	○	
개인정보보호 교육계획의 수립 및 시행	○	
개인정보파일의 보호 및 관리, 감독	○	
개인정보처리방침의 수립, 변경 및 시행	○	
개인정보보호 관련 자료의 관리	○	
처리목적이 달성되거나 보유기간 지난 개인정보의 파기	○	개인정보 취급자 이행 및 관리 감독
※ 점검결과 범례 : ○ : 적정, △ : 보완필요, × : 부적정		

- **[관련 업무의 수행]** 개인정보 보호 계획 수립 및 처리실태, 관행의 정기적인 조사, 개선 등에 대한 활동이 수행되고 있지 않음

<의견>

- 개인정보 보호 계획 수립 및 처리실태, 관행의 정기적인 조사, 개선 등에 대한 활동이 정기적으로 수행되어야 함

침해요인

- 개인정보 보호책임자의 역할 및 책임은 내부관리계획, 개인정보보호지침 등 문서로 정의되어 승인되어야 함
- 개인정보 보호책임자는 법령 등에서 부여한 역할 및 책임을 실질적으로 수행하여야 하며, 내부관리체계 강화를 위하여 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받아야 함
- 법령 등 위반사실을 알게 된 경우 즉시 개선조치를 하여야 하며, 필요 시 해당 기관장에게 개선 조치를 보고하는 등 실질적 활동이 수반되지 않으면 개인정보 보호책임자의 역할 규정에 위배될 수 있음

구분	미이행	질의코드	1.2.2	준거성여부	의무
질의문	● 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상 점검·관리하고 있습니까?				
평가근거 및 의견	**<평가>** ● 법무부 인천공항출입국·외국인청은 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상 점검·관리하고 있지 않음				

	● 개인정보보호 연간 계획 수립 등 현황 구분 / 점검결과 / 비고 연1회 이상 내부관리계획 이행 실태 점검 여부 - 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 / × / 점검결과, 개선계획 및 조치 등에 대한 문서화 여부 / × / ※ 점검결과 범례 : ○ : 적정, △ : 보완필요, × : 부적정 **<의견>** ○ 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상 점검·관리하여야 함
침해요인	● 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등은 시스템 보호 및 보안 측면에서 매우 중요하며 이에 대한 이행 실태 점검 및 관리가 되지 않을 경우, 개인정보 침해사고가 발생할 위험이 높아짐

구분	부분이행	질의코드	1.2.3	준거성여부	의무
질의문	● 개인정보보호 교육, 실태점검 등 개인정보 보호 활동에 대한 연간 수행계획을 수립·시행하고 있습니까?				
평가근거 및 의견	**<평가>** ● 법무부 인천공항출입국·외국인청은 매년 개인정보 보호활동에 대한 연간 수행계획을 수립·시행하고 있으나, 개인정보보호 조직, 인력에 대한 계획(조직구성 및 발령 등)은 다소 미흡함 ● 개인정보보호 연간 계획 수립 등 현황 구분 / 점검결과 / 비고 개인정보보호 연간계획 수립 및 내부절차를 통한 승인 여부 / × / 연간계획 내용: 개인정보보호 조직, 인력 / ○ / 연간계획 내용: 개인정보보호 활동계획 및 예산 / × / 연간계획 내용: 개인정보보호 실태점검 계획 (수탁자 포함) / ○ / 연간계획 내용: 개인정보보호 교육계획 / ○ / 연간계획에 따른 개인정보보호 활동 수행여부 점검 및 보고 / × / ※ 점검결과 범례 : ○ : 적정, △ : 보완필요, × : 부적정 **<의견>** ● 개인정보 보호 활동에 대한 연간 수행계획을 수립하고 연간계획에 따른 개인정보보호 활동 수행여부를 점검하여 개인정보 보호책임자에게 보고 및 공지하여야 함.				
침해요인	● 연간 개인정보보호 계획을 수립하는 이유는 개인정보 보호 활동이 임기응변식이				

	아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 하는데 목적이 있으며, 이를 위하여 경영진의 방향제시와 예산 및 인력 등의 지원이 필수적임 ● 개인정보보호 계획을 수립하지 않을 경우, 조직의 개인정보보호 활동을 수행할 수 없어 개인정보 침해사고가 발생할 수 있음

2) 대상시스템의 기술적 보호조치 침해요인

구분	미이행	질의코드	4.8.2	준거성여부	권고
질의문	● 개인정보취급자 및 정보주체의 개인정보 처리화면을 통한 개인정보 유·노출 등을 방지하기 위하여 개인정보 마스킹, 웹 브라우저 우측 마우스 버튼 제한, 임시 파일 및 캐시 통제, 카드번호 등 중요정보에 대한 복사·화면 캡쳐 방지 및 키보드해킹 방지 등 보호대책을 적용하도록 계획하고 있습니까?				
평가근거 및 의견	<평가> ● 대상시스템 구축 사업은 기타 기술적 안전조치로 개인정보 처리화면을 통한 개인정보 유·노출 등을 방지하기 위한 보호대책을 마련하고 있지 않음 ● 기타 보호조치 현황 구분 / 현황 / 점검결과 중요정보 마스킹 / 외국인등록번호 마스킹 처리 / × 우측 마우스 버튼 제한 / 우측마우스 버튼 제한 적용 / × 임시파일 및 캐시생성 통제 / 마우스 백버튼 제한 미적용 / × 키보드 해킹방지 / 키보드 해킹방지 적용 / × ※ 점검결과 범례 : ○ : 적정, △ : 보완필요, × : 부적정 <의견> ● 개인정보취급자가 업무 처리 시 화면을 통한 개인정보 유노출 방지를 위해 중요정보 마스킹 처리, 웹 브라우저 우측 마우스 버튼 제한, 임시 파일 및 캐시 통제, 키보드해킹방지 솔루션 적용을 권고함.				
침해요인	개인정보 처리화면을 통한 개인정보 유·노출 등 보호조치 미흡시에 처리화면을 통한 개인정보 유/노출 위험이 증가함.				

3) 특정IT 기술 활용 시 개인정보보호

구분	미이행	질의코드	5.3.1	준거성여부	의무
질의문	● 수집된 생체인식 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하도록 계획하고 있습니까?				
평가근거 및 의견	<평가> ● 바이오정보전문분석(BASE)은 신규 알고리즘의 도입을 통한 바이오 정보 수집 및 인식률				

	의 향상, 생체정보 검색·분석의 정확성 제고를 목표로 하며 해당 DB 내 생체인식 원본정보와 제공자의 신상정보가 같이 저장되어 있음 <의견> ● 개인정보취급자가 업무 처리 시 화면을 통한 개인정보 유노출 방지를 위해 중요정보 마스킹 처리, 웹 브라우저 우측 마우스 버튼 제한, 임시 파일 및 캐시 통제, 키보드해킹방지 솔루션 적용을 권고함.
침해요인	생체인식 원본정보는 변경이 불가능하다는 특성으로 인해 유출 시 다른 정보에 비해 위험성이 크며 생체인식 원본정보와 그 제공자를 알 수 있는 정보를 함께 보관하는 경우 유출 시 프라이버시 침해의 정도가 매우 더욱 커짐

다. 개선계획

1) 대상기관 개인정보보호 관리체계

[대상기관 개인정보보호 관리체계 개선계획]

우선순위	개선과제명 <법적준거성>	개선내용	담당부서	수행시기
1	개인정보보호 경력의 법적기준 요건에 충족하는 개인정보 보호책임자 지정 (1.1.1, 1.1.2) **<의무>**	① 인사발령 및 업무분장표 등을 통한 개인정보보호 전담 조직을 구성하고 개인정보보호 업무 책임 부여 ② 법에서 요구하는 경력인정 요건에 맞는 개인정보 보호책임자 지정 ③ 대표홈페이지 등에 대상기관의 개인정보보호책임자 공개 ④ 개인정보 보호책임자의 역할, 책임 정책화 및 업무 수행	총무과	2025.1
2	내부관리계획의 이행실태 점검 및 연간 개인정보보호계획의 수립·시행 (1.2.2, 1.2.3) **<의무>**	① 내부관리계획의 이행 실태 점검을 연 1회 이상 실행 ② 연간 개인정보보호 계획의 수립·시행	총무과	2025.1

2) 대상시스템의 기술적 보호조치

[대상시스템의 기술적 보호조치 개선계획]

우선순위	개선과제명 <법적준거성>	개선내용	담당부서	수행시기
1	개인정보 처리화면 보호조치 (4.8.2) **<권고>**	① 개인정보 처리화면 보호조치 - 우측마우스 버튼 제한 조치 적용 - 브라우저 캐시생성 및 임시파일 통제 (백버튼 통제, No-Cache 설정) - 키보드 해킹방지 솔루션 적용	정보관리과	2025.3

3) 특정IT 기술 활용 시 개인정보보호

[대상시스템의 기술적 보호조치 개선계획]

우선 순위	개선과제명 <법적준거성>	개선내용	담당부서	수행 시기
1	원본정보와 제공자 신원정보 분리 보관 (5.3.1) **<의무>**	① 민감한 생체인식 원본정보는 성명, 연락처, 주소 등 제공자를 알 수 있는 정보와 분리하여 별도의 저장장치에 보관(물리적 분리) - 물리적 분리가 여의치 않아 동일한 저장공간 내에 보관할 경우 별도 DB로 분리하여 침해위험을 최소화해야 함(논리적 분리)	정보관리과	2025.1