대외유출 주의

이 보고서는 행정안전부의 개인정보 영향평가 결과자료입니다. 외부에 공개되지 않도록 유의해 주시기 바랍니다.

행정안전부

KLID 한국지역정보개발원

행정안전부

고향사랑 기부제 종합정보시스템 개인정보영향평가 보고서

2023. 6.

KISM (주)한국전산감리원
Korea Information Supervision & Management

행정안전부 귀하

㈜한국전산감리원은 한국지역정보개발원과 체결한『고향사랑 기부제 종합정보시스템 개인정보 영향평가』계약에 의거하여 고향사랑 기부제 종합정보시스템에 대한 개인정보 영향평가를 실시하고, 본 개인정보 영향평가 보고서를 제출합니다.

2023년 6월 30일

㈜한국전산감리원 대표이사 최 규 택 (인)

총괄평가원 : 김 종 훈 (제2020-006호)
평가수행원 : 노 진 섭 (제2016-141호)

[개정 이력]

Ver.	작성일	변경내용	작성자	승인자
0.9	2023. 04. 26.	초안 작성	노진섭	김종훈
1.0	2023. 06. 30.	기관 검토 및 품질검토 후 확정	노진섭	김종훈

[개인정보 영향평가 보고서 개요]

<table>
<tr><td colspan="2">공공기관명</td><td colspan="4">행정안전부</td></tr>
<tr><td rowspan="6">평가대상시스템 개요</td><td>시스템명</td><td colspan="2">고향사랑 기부제 종합정보시스템</td><td>추진 일정</td><td>2023.03.06. ~
2023.05.04</td></tr>
<tr><td>추진개요 및 목적</td><td colspan="4">○ 국민이 기부 희망 지자체에 직접 기부할 수 있는 기회를 제공하여 열악한 지방재정에 대한 국비 지원의 한계를 극복하고 열악한 지방재정 보완에 직접적으로 기여</td></tr>
<tr><td rowspan="3">추진 성격</td><td>대상 여부</td><td>• 개인정보보호법 시행령 제35조 제1호 5만명 이상 민감정보・고유식별정보 처리
• 개인정보보호법 시행령 제35조 제2호 50만명 이상 개인정보파일 연계</td><td rowspan="2">추진예산</td><td rowspan="2">5,147백만원
(부가세 포함)</td></tr>
<tr><td>추진 주체</td><td>행정안전부</td></tr>
<tr><td>추진 근거</td><td>고향사랑 기부금에 관한 법률 제7조,
고향사랑 기부금에 관한 법률 시행령 제4조</td><td>비고</td><td>• 신규 구축·개발</td></tr>
<tr><td>주요 내용</td><td colspan="4">○ 기부금 시스템 구축
- 대국민 사용자 환경 구축 (기부 신청, 답례품 신청, 세액공제, 통합 이용 내역 등)
- 실명 소재지 기반의 본인인증, 기부 포인트를 활용한 답례품 구매
- 기부자 웹, 모바일 서비스, UI/UX 및 HTML5 환경 구축
- 기부 영수증, 세액공제 자동처리, 배송 현황정보 조회, 명예 기부자 커뮤니티 생성관리, 민원 처리·챗봇
- 이용자와 운영부서 의견수렴 및 반영을 위한 수시 지원체계 운영
○ 공통업무 운영관리 시스템
- 사용자 인증, 기부 포인트 조회 등 공통시스템 구축
- 지자체, 중앙부처, 답례품 등록자 등의 대상별 업무 시스템 구축
- 오프라인 수납 처리 기능, 고향사랑 기부제 종합정보시스템의 운영관리 기능 구축, 시스템 활용 성과관리 등</td></tr>
</table>

<table>
<tr><td rowspan="4">개인정보파일 개요</td><td>개인정보 수집 목적</td><td colspan="3">○ 고향사랑 기부금의 접수
○ 기부자에 대한 지자체장 명의의 기부 영수증 발급
○ 기부자에 대한 답례품 제공, 고향사랑 기부금 기탁서 확인</td></tr>
<tr><td rowspan="2">평가대상 파일</td><td>파일명</td><td>정보주체 수</td><td>파일 및 범위 설명</td></tr>
<tr><td>고향사랑e음 회원정보</td><td>131,675명</td><td>고향사랑 기부제 종합정보시스템을 이용하기 위하여 홈페이지 회원(일반회원, 답례품 공급자)으로 가입한 이용자</td></tr>
<tr><td>주요 개인정보 수집 현황</td><td colspan="3">[고향사랑e음 회원정보] 총 (18)개 항목
- 필수 수집 : 이름, 생년월일, 집주소, 휴대폰번호, ID, 비밀번호, E-Mail, 본인인증정보, 주민등록번호/외국인등록번호, 거주상태, 성별, 전자납부번호, 위반사유, 기부정보, 계좌정보, 가상계좌
- 선택 수집 : 관심지자체정보, 관심답례품정보
※ 상세한 개인정보 파일 현황은 본 보고서 21~22페이지</td></tr>
<tr><td rowspan="4">영향평가 항목</td><td rowspan="4">주요 평가항목 변경 내역</td><td>구 분</td><td colspan="2">주요내용</td></tr>
<tr><td>지표추가 항목</td><td colspan="2">- 없음</td></tr>
<tr><td>지표 변경 항목</td><td colspan="2">- 대상시스템 기술적 보호조치(4장) : 접속기록의 보관 및 점검 분야 3개 항목(4.4.1 ~ 4.4.3)은 2021년 9월 개정된 '개인정보 안전성 확보조치 기준 고시'를 반영하여 지표를 변경함</td></tr>
<tr><td>지표삭제 항목</td><td colspan="2">- 1. 대상기관 개인정보보호 관리체계(1장) 4개 평가 분야 9개 항목은 2022년 10월에 ''국가기준데이터 관리체계 구축(5차)" 개인정보 영향평가에서 시행하여 본 영향평가에서 제외함
- 5. 특정 IT 기술 활용 시 개인정보보호(5장) 4개 평가 분야 16개 항목은 평가 대상과 연관이 없어 평가에서 제외함</td></tr>
<tr><td rowspan="2">평가결과 및 개선계획</td><td rowspan="2">평가결과 및 개선사항</td><td>주요내용</td><td colspan="3">■ 평가 대상과 관련 없는 항목(해당 없음) 5개 항목을 제외하고, 총 55개 항목을 평가하였음
■ 개인정보 침해요인을 도출한 결과 대상시스템의 개인정보보호 관리체계, 개인정보 처리단계별 보호조치는 식별된 침해요인이 없었고, 대상시스템의 기술적 보호조치에서 침해요인이 1건 식별되어 총 1건의 개인정보 침해요인을 도출하였음
([별첨] 개인정보 영향평가 항목(평가표) 참조)
■ 도출한 침해요인을 기준으로 위험도 산정을 하고 개인정보 자산에 대해 위험을 감소시키기 위해 시스템 침해요인별 개선방안을 도출하였음
■ 도출된 침해요인 총 1건에 대하여 개선이 필요함</td></tr>
<tr><td>개선사항</td><td>구분</td><td>침해요인 도출 건수</td><td>개선대책 도출 건수</td><td>개선계획 수립 건수</td><td>조치 완료 건수</td><td>조치 예정 건수</td></tr>
<tr><td></td><td></td><td></td><td>고향사랑 기부제 종합정보시스</td><td>1건</td><td>1건</td><td>1건</td><td>0건</td><td>1건</td></tr>
</table>

			템				
	주요 개선계획 및 일정		**1. 대상기관의 개인정보보호 관리체계 개선** - 평가 대상 제외 **2. 대상시스템의 개인정보보호 관리체계 개선** - 해당없음 **3. 개인정보 처리단계별 보호조치 개선** - 해당없음 **4. 대상시스템의 기술적 보호조치 개선** **■ 장기 개선(6개월 이상) : 2023.05 ~ 2024.04** - 비정상적인 접근 방지 기능 구현 (4.1.7) **5. 특정 IT 기술 활용 시 개인정보보호** - 평가 대상 제외				
	평가기관		**㈜한국전산감리원**	**평가기간**	2023. 03. 06 ~ 2023. 05. 04	**평가예산**	67,163,800원 (VAT 포함)

[평가 결과 요약]

○ 행정안전부 고향사랑 기부제 종합정보시스템 영향평가를 수행한 결과는 다음과 같음

○ 행정안전부 고향사랑 기부제 종합정보시스템에 대한 점검결과, 총 60개 평가항목 중 이행 54개, 부분이행 1개, 미이행 0개, 해당없음 5개로 평가되었으며, 해당없음을 제외한 55개 항목의 이행률은 **99%**로 확인되었음

○ "영향평가 점검표"를 기준으로 3개 평가영역, 17개 평가 분야, 60개 평가항목을 점검한 결과는 다음과 같음

[도표 요약-1] 평가 결과 요약

구 분	이행	부분 이행	미이행	해당 없음	합계
1. 대상기관 개인정보 보호 관리체계	-	-	-	-	-
2. 대상시스템 개인정보 보호 관리체계	6	0	0	0	6
3. 개인정보 처리단계별 보호	17	0	0	4	21
4. 대상시스템의 기술적 보호조치	31	1	0	1	33
5. 특정 IT기술 활용 시 개인정보보호	-	-	-	-	-
합계	**54**	**1**	**0**	**5**	**60**

※ 1장 대상기관 개인정보 보호 관리체계, 5장 특정 IT 기술 활용 시 개인정보보호 평가항목 평가 제외

○ 개인정보 영향평가의 기준에 따라 행정안전부 고향사랑 기부제 종합정보시스템의 주요 개선 사항은 다음과 같음

[도표 요약-2] 개선사항 요약

(즉시: 1개월 이내, 단기: 3개월 이내, 중기: 6개월 이내, 장기: 6개월 이상)

영역	순번	개선과제 (질의문 코드)	개선내용	이행 구분	수행 주체	시기
4. 기술적 보호조치	1	비정상적인 접근 방지 기능 구현 (4.1.7)	관리자 등 특수권한 로그인 시 알림 기능 등 개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위한 대책을 마련하여 적용할 것을 권고함	권고	행정안전부	장기 (2023.05 ~ 2024.04)

[목차]

I. 추진개요	1. 사업명 ····· 2 2. 사업 목표 ····· 2 3. 평가 기간 ····· 2 4. 평가 대상 ····· 2 5. 평가 계획 ····· 4 6. 영향평가 수행인력 및 비용 ····· 17
II. 개인정보파일 개요	1. 개인정보파일 개요 ····· 21
III. 개인정보 흐름분석	1. 필요성 검토 결과 ····· 24 2. 평가자료 수집 ····· 26 3. 업무 흐름 분석 ····· 29 4. 업무흐름도 ····· 34 5. 개인정보 흐름표 ····· 36 6. 개인정보 흐름도 ····· 43 7. 시스템 구성도 ····· 47 8. 정보보호 시스템 목록 ····· 48
IV. 개인정보 영향평가 결과	1. 영향평가 항목점검 결과 ····· 50 2. 평가영역별 결과 ····· 55 3. 침해요인 도출 ····· 70
V. 위험평가	1. 위험평가 개요 ····· 73 2. 위험도 산정 결과 ····· 78 3. 개선방안 도출 ····· 80 4. 개선계획 수립 ····· 81
VI. 총 평	1. 총평 ····· 85 2. 후속 조치 ····· 87
VII. 붙 임	1. 개인정보 영향평가 품질검토 체크리스트 ····· 89
VIII. 별 첨	1. 개인정보 영향평가 항목(평가표) ····· 92

I. 추진개요

1. 사업명

○ 행정안전부 고향사랑 기부제 종합정보시스템 개인정보영향평가

2. 사업 목표

○ "행정안전부 고향사랑 기부제 종합정보시스템"에 대해 영향평가를 시행하여 잠재 위험을 식별하고 침해요인 분석을 통해 대상시스템에 대한 개선방안을 도출하여 국민의 프라이버시에 미치는 중대한 영향을 사전에 파악하고 최소화하는 데 목적이 있음

3. 평가 기간

○ 평가 기간 : 2023년 3월 6일 ~ 2023년 5월 4일 (약 2개월)

4. 평가 대상

4.1. 평가 대상시스템

평가 대상 시스템	단위 업무	개인정보 처리 구분	평가 대상 여부
고향사랑 기부제 종합정보시스템	기부금 관리	수집/보유·이용/제공/파기	○
	답례품 관리	수집/보유·이용/제공/파기	○

4.2. 평가영역

○ 1. 대상기관 개인정보 보호 관리체계
○ 2. 대상시스템의 개인정보 보호 관리체계
○ 3. 개인정보 처리단계별 보호조치
○ 4. 대상시스템의 기술적 보호조치
○ 5. 특정 IT 기술 활용 시 개인정보보호

※ 1. 대상기관의 개인정보보호 관리체계(제1장) : 2022년도 "국가기준데이터 관리체계 구축(5차)" 개인정보영향평가 사업에서 수행(2022.10)하였으므로 본 평가에서 제외함
2. 특정 IT 기술 활용 시 개인정보보호(제5장) : 평가 대상과 해당 사항이 없어 평가에서 제외함

4.3. 대상시스템의 개요

[도표 I-4.1] 사업 개요서

1. 사업(시스템)명 : 행정안전부 고향사랑 기부제 종합정보시스템

2. 시스템 운영 주체
   - 주관기관 : 행정안전부
   - 주관부서 : 지방자치균형발전실

3. 사업추진 목표
   - 최근 인구감소 등으로 지방의 재정 여건이 악화되고 수도권과 재정 격화가 심화됨에 따라 지방재정의 보완 방안 및 지역경제 활성화의 필요성 대두
   - 이를 위해, 대통령소속 자치분권위원회는 지방분권을 추진하고, 개인이 희망 지자체에 직접 기부할 수 있는「고향사랑 기부제」도입

4. 시스템 개발(구축) 일정 : 2022년 7월 ~ 2023년 7월

5. 사업 내용
   5.1 추진 배경 및 필요성
   - (재방 재정 기여) 국민이 기부 희망 지자체에 직접 기부할 수 있는 기회를 제공하여 열악한 지방재정에 대한 국비 지원의 한계를 극복하고 열악한 지방재정 보완에 직접적으로 기여
   - (기부 관리 일원화) 기부금 투명성에 대한 국민적 불신을 해소하기 위해 국가 차원의 정보시스템 구축을 통한 제도 및 시스템 운영·관리의 일원화 필요
   - (사용자 중심 포털) 행정업무 효율화 및 대국민 서비스 개선을 위해 원스톱 사용자 중심 기부 종합정보시스템 구축 필요

   5.2 서비스 내용
   - 기부금 시스템 구축
   - 공통업무 운영관리 시스템 구축
   - 7개 내·외부 시스템 연계
   - 온프레이스 인프라
   - 네트워크 구성
   - 활성화 방안
   - 서비스 운영방안

5. 평가 계획

○ 행정안전부 고향사랑 기부제 종합정보시스템에 대한 개인정보 영향평가 수행을 위해 개인정보 영향평가 운영계획을 수립함

5.1. 영향평가팀 운영계획 수립

○ 영향평가 수행기관인 (주)한국전산감리원에서 대상시스템에 대한 영향평가를 수행함

[도표 I-5.1] 개인정보 영향평가 운영계획서

<table>
<tr><th colspan="2">구분</th><th colspan="4">내용</th></tr>
<tr><td colspan="2">대상사업명</td><td colspan="4">행정안전부 고향사랑 기부제 종합정보시스템 개인정보영향평가</td></tr>
<tr><td colspan="2">평가기간</td><td colspan="4">2023. 3. 6 ~ 2023. 5. 4</td></tr>
<tr><th colspan="6">개인정보 영향평가팀(TFT) 구성</th></tr>
<tr><th colspan="2">구분</th><th>소속</th><th>성명</th><th>담당업무</th><th>역할</th></tr>
<tr><td rowspan="3">행정안전부</td><td>주관부서</td><td>지방자치균형발전실
균형발전제도과</td><td>권재철 사무관</td><td>사업 총괄</td><td>- 착수 회의, 종료 회의 등 공식 회의 참여
- 요청사항에 대한 의사 결정
- 평가를 위한 요청자료 수집 및 제공
- 인터뷰 참여
- 평가 계획, 평가 결과 검토
- 산출물에 검토 및 의견제시 등</td></tr>
<tr><td rowspan="2">유관부서</td><td rowspan="2">데이터정보화 담당관</td><td>정다산 주무관</td><td>개인정보보호 총괄</td><td rowspan="2">- 평가를 위한 요청자료 제공
- 평가 결과 검토 및 의견제시</td></tr>
<tr><td>최승재 주무관</td><td>개인정보보호 담당자</td></tr>
<tr><td colspan="2" rowspan="3">한국지역정보개발원</td><td>지역상생부</td><td>이호섭 부장</td><td>사업관리</td><td rowspan="3">- 착수 회의, 종료 회의 등 공식 회의 참여
- 요청사항에 대한 의사 결정
- 평가를 위한 요청자료 수집 및 제공
- 인터뷰 참여
- 평가 계획, 평가 결과 검토
- 산출물에 검토 및 의견제시 등</td></tr>
<tr><td>지역상생부</td><td>조병희 수석</td><td>사업관리</td></tr>
<tr><td>지역상생부</td><td>신승엽 책임</td><td>사업관리</td></tr>
</table>

개발 업체	**시스템 개발**	아이크래프트 컨소시엄	송덕호 PM	사업관리자	- 개발 산출물 및 자료 제공 - 인터뷰 응대 - 단계별 산출물 검토 및 의견제시
			김용연 이사	개발 총괄	
			박상준 매니저	사업관리	
			황원종 부장	웹 기획	
			김동환 과장	지자체 지원	
			정윤철 선임	컨설팅	
평가 기관	**영향 평가 (PIA) 팀**	(주)한국 전산감리원	김종훈 (인증번호 2020-006)	영향평가 PM	- 사업관리, 품질관리 - 대상시스템의 개인정보보호 관리체계 영역 평가 - 대상시스템의 개인정보 처리단계별 보호조치 영역 평가 - 침해요인 분석, 개선방안 도출, 개선계획 수립 - 영향평가보고서 작성 - 이행점검
			노진섭 (인증번호 2016-141)	영향평가 수행원	- 개인정보 흐름 분석 - 대상시스템의 기술적 보호조치 영역 평가 - 침해요인 분석, 위험도 산정, 개선방안 도출, 개선계획 수립 - 영향평가보고서 작성 - 이행점검
상세업무 정의	영향평가팀은 대상 시스템에 대해 세부 업무별로 개인정보의 수집, 보유, 제공 등의 단계에서 개인정보 침해 요소가 예상되는 사항을 검토하여 영향평가 결과를 보고 [평가팀의 세부 역할] ○ 영향평가 PM - 영향평가 수행 총괄 - 대상시스템의 관리체계 영역 영향평가 - 대상시스템의 기술적 보호조치 영역 평가 - 영향평가 결과보고서 등 필수 산출물 작성 - 대상시스템의 침해요인 및 개선방안 도출 - 필수 산출물 품질검토 및 교육 - 대상기관 담당자 협의				

	○ 영향평가 수행원 - 대상시스템에 대한 개인정보 흐름 분석 - 대상시스템의 개인정보 처리단계별 보호조치 영역 평가 - 영향평가 결과보고서 등 필수 산출물 작성 - 대상시스템의 침해요인 및 개선방안 도출 - 산출물 품질검토 및 교육 - 대상기관 담당자 협의
운영계획	○ 영향평가팀은 영향평가 대상시스템의 평가 시 이슈 및 검토사항에 대하여 대상기관과 협의를 위해 수시 회의 운영 ○ 영향평가에 대한 충분한 의견수렴을 통해 자체 검토항목별 개선방안 도출
추진 일정계획	○ 전체 추진 일정 : 2023. 03. 06 ~ 2023. 05. 04 (약 2개월) ○ 영향평가 준비 - 사업수행 준비 및 환경구성 2023.03.06 ~ 2023.03.10 ○ 사전분석 - 영향평가 필요성 검토 2023.03.06 ~ 2023.03.10 - 영향평가 계획서 작성 2023.03.06 ~ 2023.03.10 ○ 영향평가 실시 - 평가자료 수집 및 분석 2023.03.06 ~ 2023.03.17 - 담당자 인터뷰 2023.03.20 ~ 2023.04.21 - 개인정보 흐름 분석 2023.03.13 ~ 2023.03.31 - 영향평가 점검 및 평가표 작성 2023.03.27 ~ 2023.03.31 - 개인정보 침해요인 도출 2023.03.27 ~ 2023.04.21 - 개선방안 도출 및 개선계획 수립 2023.04.17 ~ 2023.04.28 ○ 영향평가 결과정리 - 보고서 작성 및 검토 2023.04.24 ~ 2023.04.28 - 보고서 확정 및 제출 2023.05.01 ~ 2023.05.04

5.2. 영향평가 수행계획 수립

○ 평가 목적

행정안전부 고향사랑 기부제 종합정보시스템 관리과정에서 개인정보의 수집·이용·연계 또는 처리 절차상 변경으로 개인의 프라이버시 침해 및 기관의 이미지 실추, 법률 위반 등의 위험이 발생할 가능성이 있으므로 정보시스템 확대 구축 중에 개인정보 침해위험을 개선 및 방지하기 위함

○ 평가 대상

행정안전부 고향사랑 기부제 종합정보시스템

○ 평가범위

행정안전부 고향사랑 기부제 종합정보시스템을 대상으로 시스템 확대 구축사업에서 발생할 수 있는 개인정보 침해요인

○ 평가 절차

대상기관의 대상시스템에 대해서 "개인정보 영향평가 수행안내서(20년 12월 개정)" 및 개인정보보호위원회 "개인정보 영향평가에 관한 고시(2020-04호)"를 기준으로 평가기관인 (주)한국전산감리원에서 평가하였음

[도표 I-5.2] 영향평가 수행 절차

단계		수행 내용	평가방법
계획	타당성 조사	- 대상시스템이 수집/이용/보유하고 있는 개인정보에 대한 영향평가 필요성 여부 판단	- PIA 의무대상 여부 확인 - PIA 필요성 검토 질문서 확인
	평가 수행조직 구성	- 평가기관의 PIA 조직 구성 - 대상기관의 PIA 수행조직 구성 확인	- 대상기관 PIA 운영계획서 - 수행계획서 확인
	평가 계획수립	- 평가기관의 PIA 수행계획서 작성	
분석	평가자료 수집	- 대상기관의 PIA 관련 개인정보보호 법규 및 상위기관의 지침과 내부 규정 현황 검토 - 당해 사업이해와 분석을 위한 평가자료 검토	- 대상기관의 자료요청 목록 확인 - 담당자 인터뷰

	개인정보 흐름 분석	- 대상 시스템에 대한 개인정보 처리현황 산출물 타당성 및 운영 시스템 검토 - 대상 시스템에 대한 개인정보 흐름 관련 산출물 타당성 및 운영 시스템 검토	- 개인정보 처리 업무표 - 개인정보 흐름표 - 업무흐름도 - 개인정보 흐름도 - 시스템 구성도 - 담당자 인터뷰
평가	**평가 수준 진단**	- 대상시스템에 대한 평가영역별 평가항목에 따른 평가	- 대상기관의 영향평가 항목 점검표 확인 - 영향평가 항목 점검표 기준으로 영향평가 수행
	위험평가	- 대상 시스템에 대한 평가 및 침해요인에 따른 위험도 산정	- 담당자 인터뷰, 영향평가 항목점검표 및 개인정보 흐름 분석을 통한 위험평가 실시
	개선방안 도출	- 대상 시스템에서 도출된 개인정보 침해 요소 및 개선방안에 대해 위험도가 높은 순서로 개선방안에 대한 개선계획 수립	- 담당자와 개선계획 일정 인터뷰 - 평가기관의 개인정보 개선계획 수립
보고	**개선(이행) 계획 수립**	- 대상 시스템에서 도출된 개인정보 침해 요소 및 개선방안에 대해 위험도가 높은 순서로 개선방안에 대한 개선계획 수립	- 담당자와 개선계획 일정 인터뷰 - 평가기관의 개인정보 개선계획 수립
	PIA 보고서 작성	- 영향평가 결과보고서 작성	- 평가기관의 영향평가 결과보고서 작성

○ 주요 평가사항
- 대상시스템 운영 시 개인정보보호와 관련된 법적인 요건을 만족하는지 여부
- 처리하는 개인정보에 대해 개인정보 생명 주기에 침해 우려 발생 가능성 여부
- 영향평가 점검표 기준으로 영향평가 결과 주요 침해사항 여부

○ 평가 기준 및 평가항목
- 개인정보 영향평가 수행안내서(20년 12월 개정) 준용
- 본 평가기관 영향평가 수행방법론 및 대상시스템 특성에 따른 평가지표 가감
- 개인정보보호 관련 법령 및 규정 등 개정된 사항을 반영하여 평가지표 변경
- 점검표 평가항목 기준으로 침해요인 분석 후 개선계획 수립

○ 자료수집 및 분석 계획
- 영향평가팀이 대상기관의 자료요청목록 요청 및 확인 검토
- 대상기관의 부서별 요청항목

[도표 I-5.3] 자료수집 및 면담 대상 현황

부서명	담당자	요청사항	비고
행정안전부 지방자치균형 발전실	권재철 사무관	- 주 업무 인터뷰 참여 및 대상시스템 영향평가 관련 자료 제공 - 개선 결과 관련 의견제시, 개선방안 이행 - 주요 계획수립 및 진행단계별 점검 - 산출물 검수 및 승인	자료수집, 면담
한국지역정보 개발원 지역상생부	이호섭 부장 조병희 수석 신승엽 책임	- 주 업무 인터뷰 참여 및 대상시스템 영향평가 관련 자료 제공 - 개선 결과 관련 의견제시, 개선방안 이행 - 주요 계획수립 및 진행단계별 점검 - 산출물 검수 및 승인	자료수집, 면담
아이크래프트 컨소시엄	송덕호 PM 김용연 이사 박상준 매니저 황원종 부장 김동환 과장 정윤철 선임	- 업무 인터뷰 참여 및 대상 시스템 영향평가 관련 자료 제공 - 분석, 설계, 개발 관련 자료 및 증적 제출 - 담당업무 추가 요청자료 제공 - 영향평가 점검내용 검토	자료수집, 면담

○ 평가 결과 처리

- 도출된 침해요인에 대해 개선방안 수립 및 평가 기간 내 개선 조치 가능한 사항에 대해서는 개선 조치를 이행하고, 중장기적으로 이행해야 할 과제는 개선계획을 수립함
- 평가 결과에 대하여 영향평가 결과보고서를 작성하여, 대상기관의 장에게 공문으로 제출 (단계별 산출물은 영향평가 결과보고서에 취합하여 전자파일로 별도 제출함)

5.3. 평가 기준

○ 영향평가 수행안내서 "영향평가 항목"과 행정안전부의 개인정보보호 현황을 고려하여 전체 85개 평가항목 중 25개의 평가항목을 제외하여 3개 평가영역, 17개 평가 분야, 38개 세부 분야, 60개 평가항목을 기준으로 함

※ 1. 대상기관의 개인정보보호 관리체계 평가영역은 2022년 10월에 ''국가기준데이터 관리체계 구축(5차)" 개인정보 영향평가에서 시행하여 본 영향평가 대상에서 제외하였음

※ 4. 대상시스템의 기술적 보호조치 평가영역의 4.4 접속기록의 보관 및 점검 평가 분야 3개의 평가항목(4.4.1 ~ 4.4.3)은 2021년 9월 『개인정보의 안전성 확보조치 기준』의 개정된 사항을 반영하여 지표를 변경함

※ 5. 특정 IT 기술 활용 시 개인정보보호 평가영역은 평가 대상과 연관이 없어 평가에서 제외하였음

[도표 I-5.4] 평가 기준

평가영역	평가 분야	세부 분야	비고
1. 대상기관의 개인정보보호 관리체계	1.1 개인정보보호 조직	• 개인정보보호책임자의 지정 • 개인정보보호책임자 역할수행	평가제외(2)
	1.2 개인정보보호 계획	• 내부관리계획 수립 • 개인정보보호 연간계획 수립	평가제외(3)
	1.3 개인정보 침해대응	• 침해사고 신고 방법 안내 • 유출사고 대응	평가제외(2)
	1.4 정보주체권리보장	• 정보주체 권리보장 절차 수립 • 정보주체 권리보장 방법 안내	평가제외(2)
2. 대상시스템의 개인정보보호 관리체계	2.1 개인정보취급자 관리	• 개인정보취급자 지정 • 개인정보취급자 관리・감독	
	2.2 개인정보파일 관리	• 개인정보파일대장 관리 • 개인정보파일 등록	
	2.3 개인정보처리방침	• 개인정보처리방침의 공개 • 개인정보처리방침의 작성	
3. 개인정보 처리단계별 보호조치	3.1 수집	• 개인정보 수집의 적합성 • 동의 받는 방법의 적절성	
	3.2 보유	• 보유기간 산정	

평가영역	평가 분야	세부 분야	비고
	3.3 이용·제공	• 개인정보 제공의 적합성 • 목적 외 이용·제공 제한 • 제공시 안전성 확보	
	3.4 위탁	• 위탁사실 공개 • 위탁 계약 • 수탁사 관리·감독	
	3.5 파기	• 파기 계획 수립 • 분리보관 계획 수립 • 파기대장 작성	
4. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	• 계정 관리 • 인증 관리 • 권한 관리	
	4.2 접근통제	• 접근통제 조치 • 인터넷 홈페이지 보호조치 • 업무용 모바일기기 보호조치	
	4.3 개인정보의 암호화	• 저장 시 암호화 • 전송 시 암호화	
	4.4 접속기록의 보관 및 점검	• 접속기록 보관 • 접속기록 점검 • 접속기록 보관 및 백업	항목 변경(3)
	4.5 악성프로그램 등 방지	• 백신 설치 및 운영 • 보안업데이트 적용	
	4.6 물리적 접근방지	• 출입통제 절차 수립 • 반출·입 통제 절차 수립	
	4.7 개인정보의 파기	• 안전한 파기	
	4.8 기타 기술적 보호 조치	• 개발 환경 통제 • 개인정보처리화면 보안 • 출력 시 보호조치	
	4.9 개인정보처리구역 보호	• 보호구역지정	
5. 특정IT기술 활용시 개인정보보호	5.1 CCTV	• CCTV 설치 시 의견수렴 • CCTV 설치 안내 • CCTV 사용 제한 • CCTV 설치 및 관리에 대한 위탁	평가제외(5)

평가영역	평가 분야	세부 분야	비고
	5.2 RFID	• RFID 이용자 안내 • RFID 태그부착 및 제거	평가제외(7)
	5.3 생체인식정보	• 원본정보 보관 시 보호조치	평가제외(2)
	5.4 위치정보	• 개인위치정보 수집 동의 • 개인위치정보 제공시 안내사항	평가제외(2)

5.4. 영향평가 점검항목 조정

[도표 I-5.5] 평가 기준 점검항목 조정 요약

구 분	점검항목 수				비고
	조정 전	추가	제외	조정 후	
1. 대상기관 개인정보 보호 관리체계	9	-	9	0	▪ 22년 "국가기준데이터 관리체계 구축(5차)" 개인정보 영향평가에서 시행하여 평가 제외
2. 대상시스템 개인정보 보호 관리체계	6	-	-	6	
3. 개인정보 처리단계별 보호	21	-	-	21	
4. 대상시스템의 기술적 보호조치	33	-	-	33	▪ 접속기록의 보관 및 점검 분야 3개(4.4.1 ~ 4.4.3) 항목은 2021년 9월 개정된 "개인정보 안전성 확보조치 기준(고시)"을 반영하여 지표 변경
5. 특정 IT기술 활용 시 개인정보보호	16	-	16	0	▪ 평가 대상과 연관이 없어 평가 제외
합 계	**85**	**0**	**25**	**60**	

[도표 I-5.6] 평가 기준 점검항목 조정 내역 현황표

구 분	추가, 변경 또는 제외항목		추가, 변경 또는 제외 사유
	코드	내용	
항목 제외	1.1.1	개인정보 보호책임자를 법률 기준에 따라 지정하고 있습니까?	22년 "국가기준데이터 관리체계 구축(5차)" 개인정보 영향평가에서 시행하여 평가 제외
	1.1.2	개인정보 보호책임자에게 법률이 정하는 책임 및 역할이 부여되어 있으며, 관련 업무를 수행하고 있습니까?	상동
	1.2.1	개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있습니까?	상동
	1.2.2	개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행실태를 점검·관리하고 있습니까?	상동
	1.2.3	개인정보보호 교육, 실태점검 등 개인정보보호 활동에 대한 연간 수행계획을 수립·시행하고 있습니까?	상동
	1.3.1	개인정보 침해사실을 신고할 수 있는 방법을 정보주체에게 안내하고 있습니까?	상동
	1.3.2	개인정보 유출 신고·통지 절차, 긴급 연락체계, 사고 대응 조직 구성 등을 포함한 개인정보 침해사고 대응절차를 수립하여 실시하고 있습니까?	상동
	1.4.1	개인정보 열람, 정정·삭제 및 처리정지, 수집 출처 고지 등 정보주체의 요구에 대한 처리 절차를 수립하여 실시하고 있습니까?	상동
	1.4.2	정보주체의 요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하고 있습니까?	상동
항목 변경	4.4.1	개인정보처리시스템의 접속기록을 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행 업무 등 필요한 사항이 모두 기록되도록 계획하고 있습니까?	접속기록의 보관 및 점검 분야 3개 항목은 2021년 9월 개정된 "개인정보 안전성 확보조치 기준 고시"를 반영하여 지표 변경

	4.4.2	개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 정기적(월 1회 이상)으로 점검하고 있으며, 접속기록 점검 시 다운로드한 것이 발견된 경우 내부 관리계획으로 정하는 바에 따라 반드시 그 사유를 확인하도록 계획하고 있습니까?	상동
	4.4.3	개인정보처리시스템의 접속한 기록을 최소 1년(5만명 이상의 개인정보를 처리하거나 고유식별정보 또는 민감정보 처리 시 2년) 이상 보관하고 위변조 및 도난, 분실되지 않도록 별도 저장장치 등에 백업 보관하도록 계획하고 있습니까?	상동
항목 제외	5.1.1	CCTV 설치 시 관계 전문가 및 이해관계인의 의견을 수렴하도록 계획하고 있습니까?	CCTV 평가 분야의 경우 대상시스템과 연관이 없어 평가 제외
	5.1.2	CCTV 설치 후 정보주체가 이를 쉽게 인식할 수 있도록 안내판을 설치하거나 홈페이지, 이메일 등을 통해 안내하도록 계획하고 있습니까?	상동
	5.1.3	CCTV 사용 시 임의조작 및 음성녹음을 사용할 수 없도록 계획하고 있습니까?	상동
	5.1.4	CCTV 운영 시 CCTV에 대한 운영·관리방침을 수립하도록 계획하고 있습니까?	상동
	5.1.5	CCTV 관리 위탁 시 개인정보보호에 필요한 전문장비 및 기술을 갖춘 기관을 선정하도록 계획하고 있습니까?	상동
	5.2.1	RFID 태그에 기록된 개인정보를 수집하는 경우 이용자에게 통지하거나 알아보기 쉽게 표시하도록 계획하고 있습니까?	RFID 평가 분야의 경우 대상시스템과 연관이 없어 평가 제외
	5.2.2	RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 그 사실을 이용자에게 통지하거나 알기 쉽게 표기하도록 계획하고 있습니까?	상동
	5.2.3	RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제3자에게 제공할 경우 이용자의 동의를 얻도록 계획하고 있습니까?	상동
	5.2.4	RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 설치 사실을 이용자가 인식하기 쉽게 표기하도록 계획하고 있습니까?	상동
	5.2.5	구입 및 제공받은 물품에 RFID 태그가 내장 및 부착되어 있을 경우 부착 위치, 기록정보 및 기능에 대해 표시하도록 계획하고 있습니까?	상동

	5.2.6	RFID 태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하도록 계획하고 있습니까?	상동
	5.2.7	이용자의 신체에 RFID를 지속적으로 착용하지 않도록 계획하고 있습니까?	상동
	5.3.1	수집된 생체인식 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하도록 계획하고 있습니까?	생체인식정보 평가 분야의 경우 대상시스템과 연관이 없어 평가 제외
	5.3.2	원본정보의 경우 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 계획하고 있습니까?	상동
	5.4.1	개인위치정보 수집 시 정보주체 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 계획하고 있습니까?	위치정보 평가 분야의 경우 대상시스템과 연관이 없어 평가 제외
	5.4.2	개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 통보하도록 계획하고 있습니까?	상동

[도표 I-5.7] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 적용 유형

<table>
<tr><th>구 분</th><th>1만명 미만</th><th>1만명~10만명 미만</th><th>10만명~100만명 미만</th><th>100만명 이상</th></tr>
<tr><td>공공기관</td><td colspan="2" rowspan="3">유형2(표준)</td><td colspan="2" rowspan="3">유형3(강화)</td></tr>
<tr><td>대기업</td></tr>
<tr><td>중견기업</td></tr>
<tr><td>중소기업</td><td colspan="3">유형2(표준)</td><td>유형3(강화)</td></tr>
<tr><td>소상공인</td><td rowspan="3">유형1(완화)</td><td colspan="3" rowspan="2">유형2(표준)</td></tr>
<tr><td>개인</td></tr>
<tr><td>단체</td><td colspan="2">유형2(표준)</td><td>유형3(강화)</td></tr>
</table>

행정안전부는 공공기관으로 2023년 4월 25일 기준으로 개인정보파일 등록 현황을 검토한 결과, 전체 개인정보 보유량은 100,000건 이상으로 확인되어 개인정보처리자 유형은 "유형3"에 해당하므로 『개인정보의 안전성 확보조치 기준』과 관련된 평가항목은 유형3을 적용하여 평가하는 것으로 하였음

6. 영향평가 수행인력 및 비용

6.1. 영향평가 투입인력

○ 개인정보보호위원회에서 발간한 '개인정보영향평가 대가산정 가이드(2022.9.)'에 근거하여 수행업무 범위를 기준으로 한 업무별 가중치와 사업의 특성에 의해 결정되는 업무의 가중치 및 난이도를 바탕으로 컨설팅 업무량을 산정하여 비용을 산정하였음

[도표 I-6.1] 영향평가 수행인력 투입내역

평가 분야		소요일수	투입 인원	세부 일정
평가 수행 계획수립	평가 수행 계획수립	5일	2명	2023.03.06 ~ 2023.03.10
	평가팀 구성			
평가자료 수집	내부자료 분석	5일	2명	2023.03.13 ~ 2023.03.17
	외부자료 분석			
	대상시스템 관련 자료 분석			
개인정보 흐름 분석	개인정보 처리업무 현황분석	10일	2명	2023.03.20 ~ 2023.03.31
	개인정보 흐름표 작성			
	개인정보 흐름도 작성			
	시스템 구조도 작성			
개인정보 침해요인 분석	평가항목 작성	10일	2명	2023.04.03 ~ 2023.04.14
	개인정보보호조치 현황 파악			
	개인정보 침해요인 도출			
	개인정보 위험도 산정			
개선계획 수립	개선사항 도출	10일	2명	2023.04.17 ~ 2023.04.28
	개선계획 수립			
영향평가서 작성	영향평가서 작성	4일	2명	2023.05.01 ~ 2023.05.04
	영향평가서 제출			
이행점검	이행점검 수행	-	-	-

6.2. 영향평가 총업무량

[도표 I-6.2] 영향평가 총업무량

평가 절차		평가 업무량	해당 여부	반환 값
평가 수행 계획수립	평가 수행 계획수립	0.4	○	0.4
	평가팀 구성	0.2	○	0.2
평가자료 수집	내부자료 분석	0.4	○	0.4
	외부자료 분석	0.4	○	0.4
	대상시스템 관련 자료 분석	0.6	○	0.6
개인정보 흐름 분석	개인정보 처리업무 현황분석	0.8	○	0.8
	개인정보 흐름표 작성	0.6	○	0.6
	개인정보 흐름도 작성	0.8	○	0.8
	시스템 구조도 작성	0.4	○	0.4
개인정보 침해요인 분석	평가항목 작성	0.8	○	0.8
	개인정보보호조치 현황 파악	1.2	○	1.2
	개인정보 침해요인 도출	0.6	○	0.6
	개인정보 위험도 산정	0.4	○	0.4
개선계획 수립	개선사항 도출	0.4	○	0.4
	개선계획 수립	0.6	○	0.6
영향평가서 작성	영향평가서 작성	0.8	○	0.8
	영향평가서 제출	0.4	○	0.4
이행점검	이행점검 수행	0.2	○	0.2
합계		10	-	10
총업무량 산출		10		

6.3. 영향평가 수행 비용

[도표 I-6.3] 영향평가 수행 비용

구분	내용	적용 값	비고
총업무량	총업무량 산출 값	10	
사업유형	① 구축 시스템: 1.0 ② 운용 시스템: 1.2 ③ 변경 시스템(개인정보처리 흐름 변동 없을 시): 0.8 ④ 변경 시스템(개인정보처리 흐름 추가 시): 1.0	1.0	
시스템 유형	① 단일 개인정보처리시스템 1(단일 개인정보 처리 시스템 + 특정 부서 제한 취급): 0.8 ② 단일 개인정보처리시스템 2(단일 개인정보 처리 시스템 + 2개 이하의 내부 응용 시스템): 1.0 ③ 단일 개인정보처리시스템 3(단일 개인정보 처리 시스템 + 3개 이상의 내부 응용 시스템): 1.2 ④ 복합 개인정보처리시스템 1(2개 이상의 단일 개인정보 처리 시스템 + 내부 처리): 1.4 ⑤ 복합 개인정보처리시스템 2(2개 이상의 단일 개인정보 처리 시스템 + 2개 이하의 외부 기관 응용 시스템과의 연계): 1.6 ⑥ 복합 개인정보처리시스템 3(2개 이상의 단일 개인정보 처리 시스템 + 3개 이상의 외부 기관 응용 시스템과의 연계): 1.8	1.6	
시스템 개수	① 단일시스템: 1.0 ② 복수시스템: 시스템 개수 × 0.7	1.0	
개인정보 영향평가 경험 구분	① 발주 대상 시스템과 관계없이 발주 기관의 마지막 평가 이후 1년 이내 경과: 0.8 ② 평가 대상 시스템에 대한 타 기관 또는 발주 기관의 마지막 평가 이후 1년 이내 경과: 0.7 ③ 평가기관 또는 평가 대상 시스템에 대한 마지막 평가 이후 1년 초과 경과: 0.8 ④ 평가 대상 시스템에 대한 평가 관련 정보가 확인되지 않거나 발주 기관 및 대상 시스템에 대한 평가 경험이 없는 경우: 1.0	0.8	
업무단가	정보보호 컨설턴트 평균임금	9,805,744	
컨설팅 업무량	총업무량 × 사업유형 × 시스템 유형 × 시스템 개수 × 개인정보 영향평가 경험 구분	12.8	
직접경비	-	0	
소계	업무단가 × 컨설팅 업무량 + 직접경비	125,513,523	
부가세	10% 적용	12,551,352	
DC	-	70,901,076	
용역비 합계	**-**	**67,163,800**	**(단위: 원, 부가세 포함)**

II. 개인정보파일 개요

1. 개인정보파일 개요

1.1. 행정안전부 고향사랑e음 회원정보 개인정보파일 개요

[도표 II-1.1] 고향사랑e음 회원정보 개인정보파일 개요

<table>
<tr><td colspan="2">개인정보파일을 운용하는 공공기관의 명칭</td><td colspan="3">행정안전부</td></tr>
<tr><td colspan="2">부서명</td><td>균형발전제도과</td><td>취급담당자</td><td>권재철</td></tr>
<tr><td colspan="2">업무 분야</td><td colspan="3">민원</td></tr>
<tr><td colspan="2">개인정보처리시스템의 명칭</td><td colspan="3">고향사랑 기부제 종합정보시스템</td></tr>
<tr><td colspan="2">개인정보파일의 명칭</td><td colspan="3">고향사랑e음 회원정보</td></tr>
<tr><td colspan="2">개인정보파일의 운영 근거</td><td colspan="3">정보주체 동의, 고향사랑 기부금에 관한 법률 시행령 제11조(고유식별정보의 처리)</td></tr>
<tr><td colspan="2">개인정보파일의 운영 목적</td><td colspan="3">고향사랑 기부금의 접수, 기부자에 대한 지자체장 명의의 기부 영수증 발급, 기부자에 대한 답례품 제공, 고향사랑 기부금 기탁서 확인 등</td></tr>
<tr><td colspan="2" rowspan="2">개인정보파일에 기록되는 개인정보의 항목</td><td colspan="3">1) 정보주체
필수 : 이름, 생년월일, 주소, 핸드폰(연락처), E-Mail, 회원ID, 비밀번호, 본인인증정보
선택 : 관심지자체정보, 관심답례품정보, 기부지자체, 기부금액, 납부자번호, 전자납부번호, 위반사유, 계좌정보</td></tr>
<tr><td colspan="3">2) 법정대리인
필수 : 이름, 생년월일, 주소, 핸드폰(연락처), E-Mail, 회원ID, 비밀번호, 본인인증정보
선택 : 관심지자체정보, 관심답례품정보, 기부지자체, 기부금액, 납부자번호, 전자납부번호, 위반사유</td></tr>
<tr><td colspan="2">개인정보의 처리 방법</td><td colspan="3">개인정보처리시스템(고향사랑e음 시스템)</td></tr>
<tr><td colspan="2">개인정보의 보유기간</td><td colspan="3">회원 탈퇴 시까지 또는 2년</td></tr>
<tr><td rowspan="3">개인정보를 통상적 또는 반복적으로 제공하는 경우</td><td>제공받는 자</td><td colspan="3">국세청</td></tr>
<tr><td>근거</td><td colspan="3">1) 고향사랑 기부금에 관한 법률 제8조(고향사랑 기부금의 접수 및 상한액)제1항 및 같은 법 시행령 제4조(고향사랑 기부금의 접수 방법 및 절차)제1항
2) 소득세법 시행령 제118조의7(기부금의 세액공제 등)
3) 지방세징수법 시행령 제29조(납부 및 수납의 방법)</td></tr>
<tr><td>개인정보의 범위</td><td colspan="3">납부자번호, 이름, 핸드폰(연락처), E-Mail</td></tr>
<tr><td colspan="2">개인정보파일로 보유하고 있는 개인정보의 정보주체 수</td><td colspan="3">131,675명</td></tr>
<tr><td rowspan="2">해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서</td><td>범위</td><td colspan="3">해당 업무부서의 담당자와 시스템 관리자만이 접근하여 활용할 수 있다.</td></tr>
<tr><td>공동사용 부서</td><td colspan="3">없음</td></tr>
<tr><td colspan="2">개인정보의 열람 요구를 접수, 처리하는 부서</td><td colspan="3">행정안전부 데이터정보화담당관</td></tr>
</table>

개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유	개인정보의 범위	없음
	사유	없음

III. 개인정보 흐름 분석

1. 필요성 검토 결과

1.1. 개인정보 영향평가 의무대상 여부 확인

○ 아래와 같이 행정안전부에서 운영 중인 '고향사랑 기부제 종합정보시스템'에 대한 개인정보 영향평가 의무대상 여부를 확인한 결과, 본 사업은 5만 명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반될 것으로 예상되어 법적 의무대상임

[도표 III-1.1] 개인정보 영향평가 의무대상 여부 확인

No.	질문	결과			비고
		Y	N	N/A	
1	5만 명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반될 것으로 예상됩니까?	○			
2	해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계한 결과 50 만명 이상의 정보주체에 관한 개인정보가 포함 또는 포함될 것으로 예상됩니까?	○			
3	100만 명 이상의 정보주체에 관한 개인정보파일을 처리 또는 처리가 예상됩니까?		○		
4	법 제33조제1항에 따른 개인정보 영향평가를 받은 후에 개인정보 검색 체계 등 개인정보파일의 운용 체계를 변경하려고 합니까?		○		

1.2. 개인정보 영향평가 필요성 검토 질의 결과서

○ 개인정보보호법의 시행(2011. 09. 30.)에 따라 행정안전부에서 운영 중인 '고향사랑 기부제 종합정보시스템'에 대하여 개인정보 영향평가 필요성을 검토한 결과는 아래의 도표와 같음

[도표 III-1.2] 개인정보 영향평가 필요성 검토 질의 결과서

No.	질문	결과			비고
		Y	N	N/A	
1	당해 사업이 개인정보의 수집 방법을 기존에 정보주체로부터 직접 수집하는 방식에서 타 기관(산하기관 포함)으로부터 제공받는 경우 등과 같이 수집하는 방식 등을 변경하는가?		○		
2	당해 사업의 수행을 위해 타 기관으로부터 개인정보를 제공받거나 당해 기관의 개인정보 DB를 타 기관과 연계하여 이용할 필요가 있는가?	○			
3	당해 사업의 수행을 위해 개인정보를 수집, 보유, 이용.제공, 파기하는 기존의 업무수행 절차에 중대한 변경이 초래되는가?		○		
4	기존의 정보시스템에 특정 IT 기술을 적용하는 새로운 활용법을 채택함으로써 기존에 수집되거나 향후 수집될 정보가 본인확인이 가능한 형태로 변경되는 등 시스템상에 중대한 변화가 발생하는가?			○	
5	당해 사업의 수행을 위해 개인정보 수집 등의 업무처리 절차를 변경함으로써 기존에 예상치 못한 개인정보의 사용 또는 폐기를 야기하거나 본인확인이 가능한 형태의 정보를 주기적으로 수집해야 하는 필요성이 있는가?		○		
6	서비스 이용 과정에서 생성되는 정보를 기존에 수집한 개인정보와 결합함으로써 정보주체의 프라이버시에 영향을 미칠 수 있는 2차적 정보가 생성되는가?	○			
7	당해 사업의 수행을 위해 기존에 수집된 개인정보를 개인정보 수집 시 정보주체에게 고지한 수집 목적 또는 이용목적 외로 사용할 가능성이 있는가?		○		
8	구축하고자 하는 정보시스템이 위치정보, RFID 등 특정 IT 기술을 활용한 서비스를 제공하기 위한 것으로서 정보주체의 개인정보 침해 문제가 발생할 가능성이 있다고 예측되는가?			○	
9	신규 또는 추가로 구축되는 시스템이 개인정보 DB에 대한 접근을 관리 또는 통제하기 위해 사용되는 보안체계에 중대한 변화를 초래하는가?		○		

2. 평가자료 수집

2.1. 평가자료 수집 목적 및 종류

○ 영향평가 수행에 앞서 평가 대상 및 개인정보 정책 환경을 분석하기 위한 관련 자료를 수집함
○ 분석 대상 자료는 기관 내·외부 개인정보 보호 관련 규정 및 정책 환경 등을 분석하기 위해 개인정보보호와 관련한 ①내부 정책자료, ②외부 정책자료, ③대상시스템 설명자료 등으로 구분함

2.2. 내부 정책자료

[도표 III-2.1] 내부 정책자료 목록

구분	수집 목적	수집자료	수집기관
조직체계 자료	기관 내부의 개인정보 보호체계, 규정, 조직현황 파악	- 해당기관 조직도, 업무분장표 - 행정안전부 개인정보보호 지침 - 행정안전부 개인정보보호 내부관리계획 - 행정안전부 개인정보 담당자 업무 매뉴얼 - 개인정보보호처리방침 - 개인정보 침해사고 대응 매뉴얼 - 재해 및 재난 대응 매뉴얼 - 개인정보 암호화 키 관리 절차서	행정안전부, 한국지역정보개발원
인적 보안 및 교육 자료	기관 내부의 개인정보취급자 및 위탁업체에 대한 내부규정 및 관리·교육체계 파악, 조직현황 파악	- 개인정보보호 교육계획서 및 교육 결과서 - 개인정보보호 실태점검 및 절차서 - 개인정보취급자 지정현황 - 개인정보처리 위탁업체/제3자 제공 목록 - 개인정보보호 관련 표준 위탁 계약서 - 개인정보 취급위탁 보안 서약서 - 위·수탁 협약서	행정안전부, 한국지역정보개발원
시스템 구성 및 보안 관련 자료	시스템 구조와 연계된 개인정보 보호 기술 현황 파악	- 네트워크/시스템 구성도 - 정보보호 시스템 현황 - 전산실 출입 관리대장 - 접속기록 관리 및 점검 사항 - 업무흐름도 - 서버/DB 접근제어시스템 사용자 신청서 - 웹 취약점 진단 계획서 - 웹 취약점 진단 결과서	한국지역정보개발원

2.3. 외부 정책자료

[도표 III-2.2] 외부 정책자료 목록

구분	수집 목적	수집자료	수집기관
대상기관 관련 법률	소속기관의 규정 및 지침 분석	- 공공기록물 관리에 관한 법률/시행령 - 전자정부법/시행령 - 민원처리에관한법률/시행령/시행규칙 - 수혜적 공공서비스 목록 제공에 관한 지침 - 행정정보 공동이용 지침 - 행정안전부 개인정보보호 규정/지침/ 가이드 - 고향사랑 기부금에 관한 법률/시행령	행정안전부
개인정보 보호 관련 지침	개인정보보호 관련 정책 및 법률 등 환경 분석	- 개인정보보호법 및 시행령·시행규칙 - 개인정보 보호법령 및 지침·고시 해설서 - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령 - 표준 개인정보 보호지침 - 개인정보 영향평가 고시 - 개인정보 영향평가 고시 해설서 - 개인정보 영향평가 수행 안내서 - 개인정보의 안전성 확보조치 기준 고시 - 개인정보의 안전성 확보조치 기준 고시 해설서 - 개인정보의 암호화 조치 안내서 - 개인정보 위험도 분석 기준 - 개인정보의 기술적·관리적 보호조치 기준 - 개인정보의 기술적·관리적 보호조치 기준 해설서 - 개인정보 처리 위·수탁 안내서 - 홈페이지 개인정보 노출방지 안내서 - 주민번호 수집금지제도 가이드라인 - 개인정보 수집 최소화 가이드라인 - 개인정보 수집제공 동의서 작성 가이드라인 - 개인정보 비식별 조치 가이드라인	㈜한국전산감리원

2.4. 대상시스템 설명자료

[도표 III-2.3] 시스템 설명자료 목록

구분	수집 목적	수집자료	수집기관
사업관리 자료	정보시스템에 의하여 수집되는 개인정보의 양과 범위가 사업수행을 위해 적절한지 파악	- 사업수행계획서 - 착수보고서 - 중간보고서 - 위험 관리계획서 - 위험 관리대장 - 요구사항 정의서 추적표 - 형상 관리계획서 - 형상 관리 결과서 - 보안 관리계획서 - 월별/일별 보안점검 - 정보보안 교육 결과서 - 보안 관리대장 - 보안 서약서 - PC 수동 점검 - 교육계획서/교육 결과서 - 아키텍처 정의서 - 업무흐름도 - 용어 정의서 - 데이터 표준 정의서 - 메뉴 목록 정의서 - 메뉴 구성도 - 사용자화면 목록 - 사용자화면 정의서 - 프로그램 목록 - 프로그램 명세서 - 데이터베이스 정의 - 테이블 정의서 - 테이블 목록 - 테스트 계획서 - 시스템 아키텍처 설계 - 데이터 전환 계획서 - 시큐어 코딩 설계서 - 설치 계획서	아이크래프트 컨소시엄
외부 연계 자료	정보시스템의 외부 연계 여부 파악	- 유관기관 시스템 조사서 - 인터페이스 목록 - 인터페이스 설계서	아이크래프트 컨소시엄

3. 업무 흐름 분석

3.1. 목적

○ 본 사업의 모든 업무가 개인정보를 처리하는 것은 아니므로, 평가 대상 사업의 업무를 분석하여 개인정보 처리가 수반되는 업무를 구분하고 각 업무에서 처리하는 개인정보를 식별함

3.2. 정보주체

○ 행정안전부에서 제공하는 고향사랑e음(고향사랑 기부제 종합정보시스템)을 이용하기 위하여 홈페이지 회원(일반회원, 답례품 공급자)으로 가입한 이용자

3.3. 개인정보취급자

○ 고향사랑e음 회원으로부터 홈페이지를 통하여 기부하는 고향사랑 기부금 및 답례품 구매를 처리하는 전국 각 지자체의 관리자(행안부 관리자 포함) 및 업무 담당자(내부 직원, 임시직, 계약직 포함)
○ 직접 방문하여 기부하는 오프라인 기탁자의 기부금 기탁서를 접수, 처리하는 전국 각 농협은행 및 농축협의 업무 담당자(내부 직원, 임시직, 계약직 포함)
○ 행정안전부로부터 시스템 구축, 운영, 유지보수 업무를 위탁받은 수탁기관 직원

3.4. 시스템 평가 범위

[도표 III-3.1] 시스템 평가 자료

분야		설명
고향사랑 기부제 종합정보시스템	기부금 관리	기부금 납부, 영수증 발급, 기부 포인트 적립 처리
	답례품 관리	답례품 공급자 심사/선정, 주문, 배송, 클레임, 정산 처리

3.5. 개인정보 처리 업무표

○ 행정안전부 고향사랑 기부제 종합정보시스템의 개인정보 처리업무는 아래와 같음
○ 고향사랑 기부제 종합정보시스템은 고유식별정보를 처리하고 있으나, 본인 거주지의 확인 용도로만 사용하고, DB에는 실명 인증값(CI)으로 대체하여 저장

[도표 III-3.2] 개인정보 처리 업무표

No	평가 업무명	처리목적	처리 개인정보	주관부서	개인정보 처리건수 (고유식별 번호건수)	개인정보 영향도
1-1	기부금 관리 (일반회원) (법정대리인 포함)	회원가입, 회원정보 변경/탈퇴, 기부금납부	**[필수]** 이름, 생년월일, 집주소, 휴대폰번호, ID, 비밀번호, E-Mail, 본인인증정보(CI, DI, DN, 디지털원패스 userkey), 주민등록번호(외국인등록번호)(주소지 확인용, 내부시스템에 보관하지않음), 거주상태, 성별, 전자납부번호(서울시Etax,지방세Wetax), 위반사유(코드, 내용) **[선택]** 관심지자체정보, 관심답례품정보	행정안전부 균형발전제도과	미정 **주1)**	5
1-2	기부금 관리 (오프라인 기탁자)	회원가입, 회원정보 변경/탈퇴, 기부금납부	**[필수]** ID, 기부자명, 주민등록번호(외국인등록번호)(주소지 확인용, 내부시스템에 보관하지않음), 휴대폰번호, 집주소, 기부지자체, 기부금액, 접수은행, 전자납부번호, 답례품 제공유무 **[선택]** 없음	행정안전부 균형발전제도과	미정	5
1-3	기부금 관리 (답례품 판매자)	답례품 판매자 등록신청, 판매, 배송,대금정산	**[필수]** ID, 비밀번호, 휴대폰번호, 이메일, 상호, 대표자명, 입금은행명, 예금주명, 입금계좌번호, 가상계좌 **[선택]** 없음	지자체 관리자	미정	5

2-1	답례품 관리 (답례품 주문자)	답례품 주문, 배송, 클레임(취소, 교환, 반품, 환불), 정산, 운영(후기, 붐), 이벤트	**[필수]** 이름, 주소, 휴대폰번호, 이메일 **[선택]** 없음	지자체 관리자	미정	3
2-2	답례품 관리 (답례품 수령자)	답례품 주문, 배송, 클레임(취소, 교환, 반품, 환불)	**[필수]** 이름, 주소, 휴대폰번호 **[선택]** 전화번호	지자체 관리자	미정	

주1) 고향사랑 기부제 종합정보시스템은 현재 개발/구축이 진행 중이므로 개인정보 건수 확인이 어려움

3.6. 개인정보 현황표

○ 행정안전부 고향사랑 기부제 종합정보시스템의 개인정보 현황표는 아래와 같음

[도표 III-3.3] 개인정보 현황표

평가 업무명	개인정보 처리항목	개인정보 세부항목	수집근거	필수/선택	수집목적
1-1 기부금관리 (일반회원) (법정대리인 포함)	이름	-	정보주체의 동의	필수	본인확인
	생년월일	-	정보주체의 동의	필수	본인확인
	집주소	-	정보주체의 동의	필수	거주지확인
	휴대폰번호	-	정보주체의 동의	필수	본인확인 및 연락
	ID	-	정보주체의 동의	필수	본인확인
	비밀번호	-	정보주체의 동의	필수	본인인증
	이메일	-	정보주체의 동의	필수	비밀번호 분실 시 본인 확인 및 연락
	본인인증정보	CI	개인식별정보 및 인증정보 암호화	필수	외부기관 송수신 시 개인식별정보 및 인증정보 암호화
		DI		필수	
		DN		필수	
		디지털원패스userkey		필수	
	주민등록번호 (외국인등록번호)	-	고향사랑기부금에 관한 법률 시행령 제11조(고유식별정보의 처리)	필수	본인 및 거주지 확인
	거주상태	-	정보주체의 동의	필수	본인 및 거주지 확인
	전자납부번호	-	정보주체의 동의	필수	기부금수납
	성별	-	정보주체의 동의	필수	통계작성
	위반사유	-	정보주체의 동의	필수	위법행위 감독
	관심지자체정보	-	정보주체의 동의	선택	기부금납부
	관심답례품정보	-	정보주체의 동의	선택	답례품구매
1-2 기부금관리 (오프라인 기탁자)	ID	-	정보주체의 동의	필수	본인확인
	기부자명	-	정보주체의 동의	필수	본인확인
	주민등록번호 (외국인등록번호)	-	고향사랑기부금에 관한 법률 시행령 제11조(고유식별정보의 처리)	필수	본인 및 거주지 확인
	휴대폰번호	-	정보주체의 동의	필수	본인확인 및 연락
	집주소	-	정보주체의 동의	필수	거주지확인
	기부지자체	-	정보주체의 동의	필수	기부지역확인

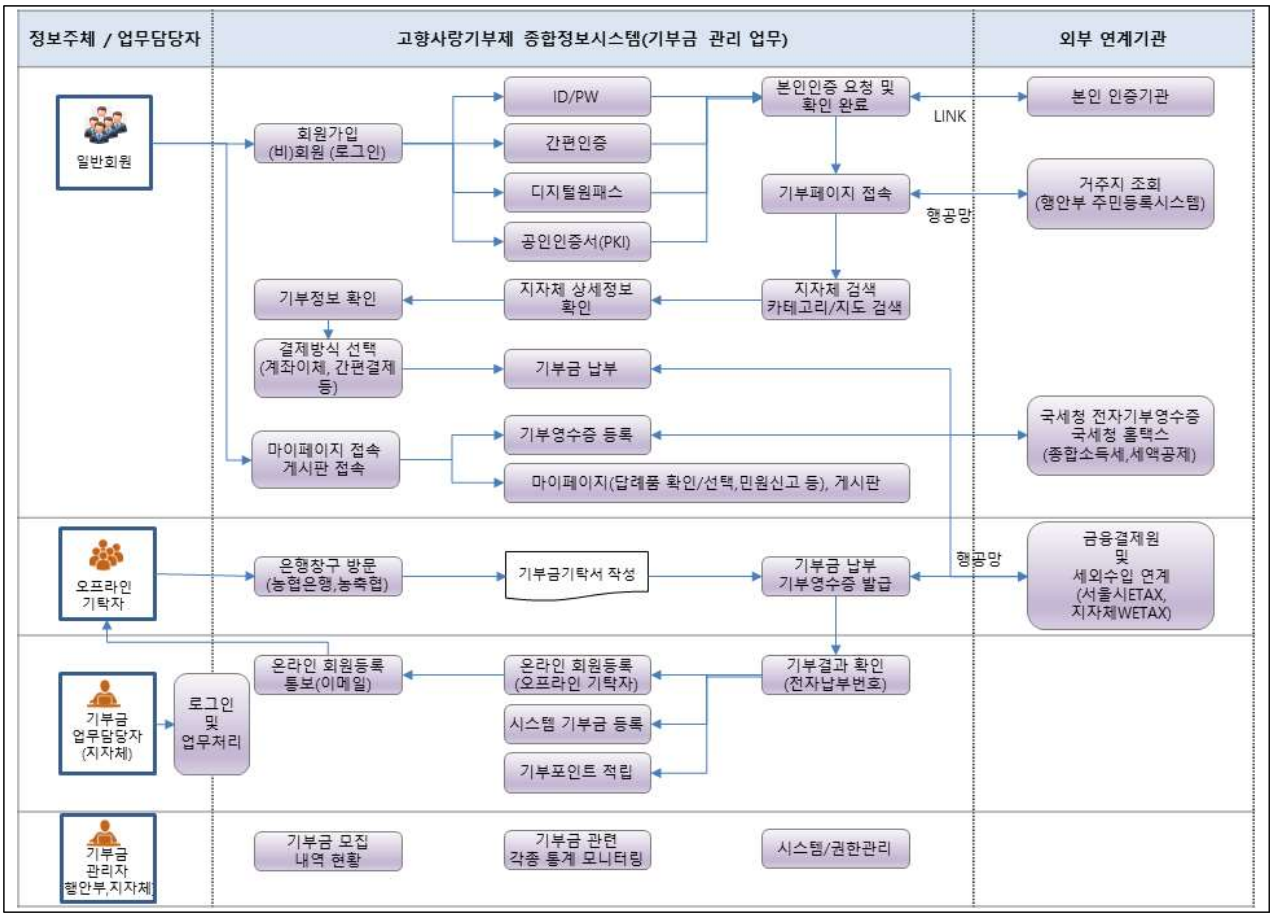
	기부금액	-	정보주체의 동의	필수	기부금수납
	접수은행	-	정보주체의 동의	필수	기부금수납
	전자납부번호	-	정보주체의 동의	필수	기부금수납
	답례품제공유무	-	정보주체의 동의	필수	답례품구매
1-3 기부금관리 (답례품 판매자)	ID	-	정보주체의 동의	필수	본인확인
	비밀번호	-	정보주체의 동의	필수	본인인증
	휴대폰번호	-	정보주체의 동의	필수	본인확인 및 연락
	이메일	-	정보주체의 동의	필수	비밀번호 분실 시 본인 확인 및 연락
	상호	-	정보주체의 동의	필수	통신판매사업자 확인
	대표자명	-	정보주체의 동의	필수	통신판매사업자 확인
	입금은행명	-	정보주체의 동의	필수	판매수익 입금
	예금주명	-	정보주체의 동의	필수	판매수익 입금
	입금계좌번호	-	정보주체의 동의	필수	판매수익 입금
	가상계좌	-	정보주체의 동의	필수	판매수익 입금
2-1 답례품관리 (답례품 주문자)	이름	-	정보주체의 동의	필수	본인확인
	주소	-	정보주체의 동의	필수	거주지확인
	휴대폰번호	-	정보주체의 동의	필수	본인확인 및 연락
	이메일	-	정보주체의 동의	필수	본인 확인 및 연락
2-2 답례품관리 (답례품 수령자)	이름	-	정보주체의 동의	필수	본인확인
	주소	-	정보주체의 동의	필수	거주지확인
	휴대폰번호	-	정보주체의 동의	필수	본인확인 및 연락
	전화번호	-	정보주체의 동의	선택	본인확인 및 연락

4. 업무흐름도

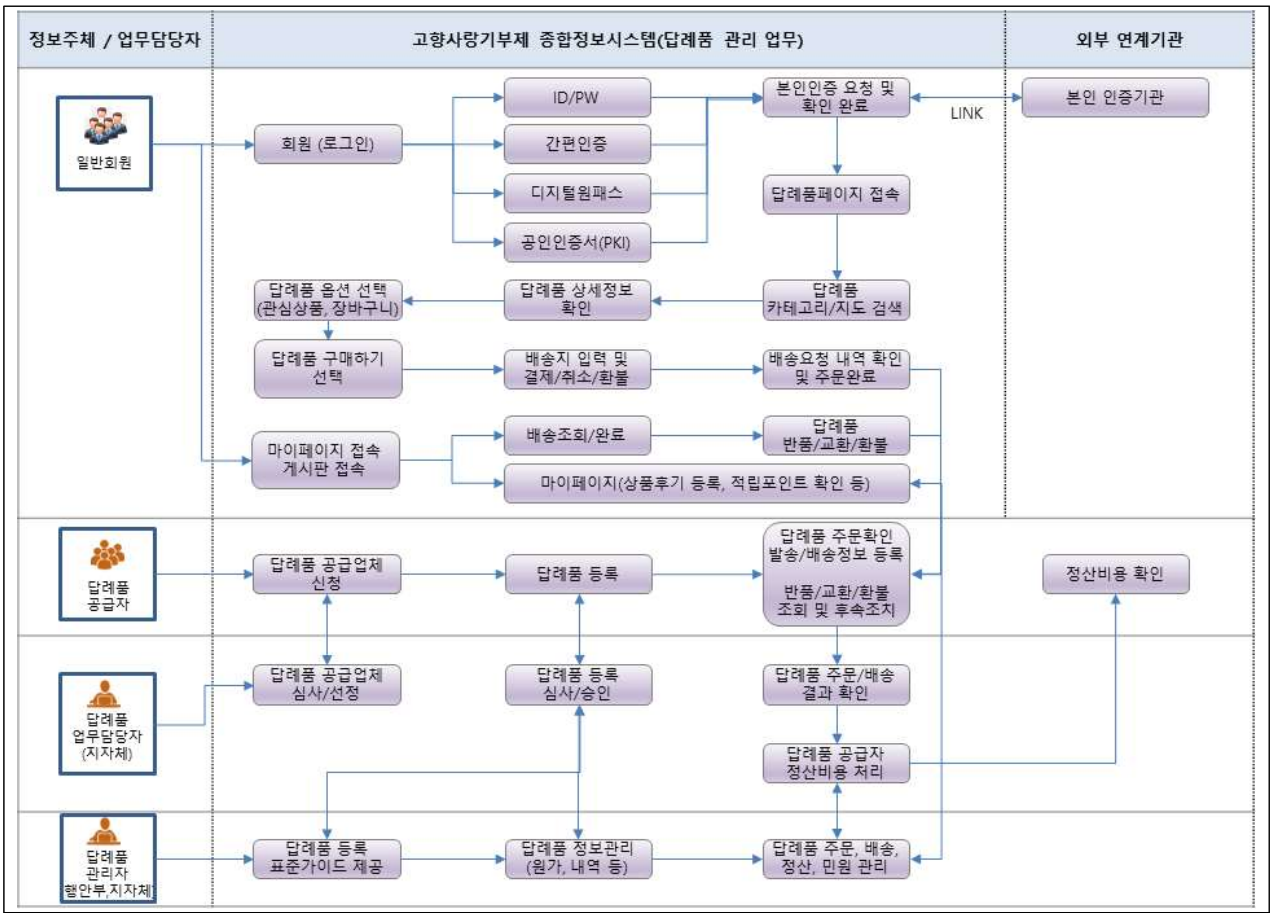
4.1. 업무흐름도

○ 행정안전부 고향사랑 기부제 종합정보시스템의 업무흐름도는 다음 그림과 같음

[도표 III-4.1] 기부금 관리 업무흐름도



[도표 III-4.2] 답례품 관리 업무흐름도



5. 개인정보 흐름표

○ 행정안전부 고향사랑 기부제 종합정보시스템의 **수집 단계** 개인정보 흐름은 아래와 같음

[도표 III-5.1] 개인정보 흐름표(수집)

N0	평가업무명	수집					
		수집항목	수집 경로	수집 대상	수집 주기	수집 담당자	수집근거
1-1	기부금관리 (일반회원)	**홈페이지 일반회원가입자 (기부자, 법정대리인)** **[필수]** 이름, 생년월일, 집주소, 휴대폰번호, ID, 비밀번호, E-Mail, 본인인증정보(CI, DI, DN, 디지털원패스 userkey), 주민등록번호(외국인등록번호)(주소지 확인용, 내부시스템에 보관하지않음), 거주상태, 성별, 전자납부번호(서울시Etax,지방세Wetax), 위반사유(코드, 내용) **[선택]** 관심지자체정보, 관심답례품정보	홈페이지 (온라인)	정보주체	수시	시스템 관리자 및 지자체 담당자	정보주체의 동의 고향사랑기부금에 관한 법률 시행령 제11조(고유식별정보의 처리)
1-2	기부금관리 (오프라인 기탁자)	**[필수]** ID, 기부자명, 주민등록번호(외국인등록번호)(주소지 확인용, 내부시스템에 보관하지않음), 휴대폰번호, 집주소, 기부지자체, 기부금액, 접수은행, 전자납부번호, 답례품 제공유무 **[선택]** 없음	농협은행, 농축협 (오프라인)	정보주체	수시	농협은행, 농축협 담당자	정보주체의 동의 고향사랑기부금에 관한 법률 시행령 제11조(고유식별정보의 처리)
1-3	기부금관리 (답례품 판매자)	**[필수]** ID, 비밀번호, 휴대폰번호, 이메일, 상호, 대표자명, 입금은행명, 예금주명, 입금계좌번호, 가상계좌 **[선택]** 없음	홈페이지 (온라인)	정보주체	수시	지자체 담당자	정보주체 동의

N0	평가업무명	수집					
		수집항목	수집 경로	수집 대상	수집 주기	수집 담당자	수집근거
2-1	답례품관리 (답례품 주문자)	**[필수]** 이름, 주소, 휴대폰번호, 이메일 **[선택]** 없음	홈페이지 (온라인)	정 보 주체	수시	지 자 체 담당자	정보주체 동의
2-2	답례품관리 (답례품 수령자)	**[필수]** 이름, 주소, 휴대폰번호 **[선택]** 전화번호	홈페이지 (온라인)	정 보 주체	수시	지 자 체 담당자	정보주체 동의

○ 행정안전부 고향사랑 기부제 종합정보시스템의 **보유·이용단계** 개인정보 흐름은 아래와 같음

[도표 III-5.2] 개인정보 흐름표(보유·이용)

No	평가 업무명	보유·이용					
		보유 형태	암호화 항목	이용항목	이용 목적	개인 정보 취급자	이용 방법
1-1	기부금 관리 (일반회원)	DB	**[SHA512]** 비밀 번호 **[ARIA256]** 본인인증정보(CI),ID,전화번호,휴대폰번호,주소,위반사유	**홈페이지 일반회원가입자(기부자, 법정대리인)** **[필수]** 이름,생년월일,집주소,휴대폰번호,ID,비밀번호,E-Mail,본인인증정보(CI,DI,DN,디지털원패스userkey),거주상태,성별,전자납부번호(서울시Etax,지방세Wetax),위반사유(코드,내용) **[선택]** 관심지자체정보,관심답례품정보	기부금납부, 회원정보 변경 및 탈퇴	시스템 관리자 및 지자체 담당자	PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 처리
1-2	기부금 관리 (오프라인 기탁자)	DB	**[ARIA256]** 본인인증정보(CI),ID,휴대폰번호,주소	**오프라인 기탁자** **[필수]** ID,기부자명,휴대폰번호,집주소,기부지자체,기부금액,접수은행,전자납부번호,답례품 제공유무 **[선택]** 없음	기부금납부, 회원정보 변경 및 탈퇴	시스템 관리자 및 지자체 담당자	PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 처리
1-3	기부금관리 (답례품 판매자)	DB	**[SHA512]** 비밀 번호 **[ARIA256]** ID,휴대폰번호, 이메일,상호, 대표자명, 입금은행명, 예금주명,	**답례품 판매자** **[필수]** ID,비밀번호,휴대폰번호,이메일,상호,대표자명,입금은행명,예금주명,입금계좌번호,가상계좌번호 **[선택]** 없음	답례품 판매자 등록 신청, 판매, 배송, 대금정산	시스템 관리자 및 지자체 담당자	PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 처리

No	평가 업무명	보유·이용					
		보유 형태	암호화 항목	이용항목	이용 목적	개인 정보 취급자	이용 방법
			입금계좌번호, 가상계좌번호				
2-1	답례품 관리 (답례품 주문자)	DB	**[ARIA256]** IP,이름,주소, 휴대폰번호, 이메일, 환불계좌주,환불계좌번호	**답례품 주문자(기부자)** **[필수]** 이름, 주소, 휴대폰번호, 이메일,환불계좌주,환불계좌번호 **[선택]** 없음	답례품 주문, 배송, 클레임(취소, 교환, 반품, 환불)	지자체 담당자	PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 처리
2-2	답례품 관리 (답례품 수령자)		**[ARIA256]** 이름, 주소, 휴대폰번호, 전화번호	**답례품 수령자(수취인)** **[필수]** 이름, 주소, 휴대폰번호 **[선택]** 전화번호	답례품 주문, 배송, 클레임(취소, 교환, 반품, 환불)	지자체 담당자	PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 처리

○ 행정안전부 고향사랑 기부제 종합정보시스템의 **제공단계** 개인정보 흐름은 아래와 같음

[도표 III-5.3] 개인정보 흐름표(제공)

No	평가 업무명	제공							
		제공목적	제공자	수신자	제공정보	제공 방법	제공 주기	제공 시 암호화	제공근거
1-1	기부금 관리 (일반 회원)	기부금 납부	고향사랑e음	서울시 세외시스템	납세자(기부자)ID, 납세자명, 납세자 구분, 휴대폰번호, 전화번호, 거주상태, 집주소	행공망	수시	구간 암호화	고향사랑 기부금에 관한 법률 제8조(고향사랑 기부금의 접수 및 상한액)제1항 및 같은 법 시행령 제4조(고향사랑 기부금의 접수 방법 및 절차)제1항
		기부금 납부	고향사랑e음	지방 세외시스템 (현세대)	납부자번호, 성명, 전화번호, 휴대폰번호, 이메일, 집주소, 은행코드	행공망	수시	구간 암호화	
		전자신고 및 납부	고향사랑e음	금융결제원 통합수납 처리센터	전자납부번호, 계좌번호, 계좌주 성명	RestFul	수시	구간 암호화	지방세징수법 시행령 제29조(납부 및 수납의 방법)
		국세청 소득세 세액공제	고향사랑e음	국세청 전자기부 영수증시스템	기부금액, 기부자 신분확인코드, 외부기관개인 식별암호화내용	Rest Api	수시	구간 암호화	소득세법 시행령 제118조의7(기부금의 세액공제 등)
		기부자 주소지 확인	고향사랑e음	행정안전부 주민등록 시스템	기부자(이름, 주민등록번호)	행공망	수시	구간 암호화	고향사랑 기부금에 관한 법률 시행령 제4조(고향사랑 기부금의 접수 방법 및 절차) 제2항 및 제3항
1-2	기부금 관리 (오프라인 기탁자)	기부금 납부	고향사랑e음	서울시 세외시스템	납세자(기부자)ID, 납세자명, 납세자 구분, 휴대폰번호, 전화번호, 거주상태, 집주소	행공망	수시	구간 암호화	고향사랑 기부금에 관한 법률 제8조(고향사랑 기부금의 접수 및 상한액)제1항 및 같은 법 시행령
		기부	고향사	지방 세	납부자번호, 성명,	행공	수시	구간	

No	평가 업무명	제공							
		제공목적	제공자	수신자	제공정보	제공 방법	제공 주기	제공 시 암호화	제공근거
		금 납부	랑e음	외시스템 (현세대)	전화번호, 휴대폰 번호, 이메일, 집 주소, 은행코드	망		암호화	제4조(고향사랑 기부금의 접수 방법 및 절차)제1항
		전자신고 및 납부	고향사랑e음	금융결제원 통합수납 처리센터	전자납부번호, 계좌번호, 계좌주 성명	RestFul	수시	구간 암호화	지방세징수법 시행령 제29조(납부 및 수납의 방법)
		국세청 소득세 세액공제	고향사랑e음	국세청 전자기부 영수증시스템	기부금액, 기부자 신분확인코드, 외부기관개인 식별암호화내용	Rest Api	수시	구간 암호화	소득세법 시행령 제118조의7(기부금의 세액공제 등)
		기부자 주소 지 확인	고향사랑e음	행정안전부 주민등록 시스템	기부자(이름, 주민등록번호)	행 공 망	수시	구간 암호화	고향사랑 기부금에 관한 법률 시행령 제4조(고향사랑 기부금의 접수 방법 및 절차) 제2항 및 제3항
1-3	기부금 관리 (답례품판매자)	-	-	-	-	-	-	-	-
2-1	답례품 관리 (답례품주문자)	-	-	-	-	-	-	-	-
2-2	답례품 관리 (답례품수령자)	-	-	-	-	-	-	-	-

○ 행정안전부 고향사랑 기부제 종합정보시스템의 **파기 단계** 개인정보 흐름은 아래와 같음

[도표 III-5.4] 개인정보 흐름표(파기)

No	평가 업무명	파기			
		보관기간	파기담당자	파기절차	분리 보관
1-1	기부금관리 (일반회원)	회원 탈퇴 시 또는 2년	업무담당자	목적 달성 시 기존 정보의 복구가 불가능하도록 해당레코드가 자동 삭제되고 있음	고향사랑기부금의 통계 수치 관리를 위한 일부 기부이력정보(기부 지자체 정보, 기부금액, 기부일자, 연령대)는 이관하여 다른 개인정보와 분리하여 별도 DB에 저장·관리하도록 계획하고 있음
1-2	기부금관리 (오프라인 기탁자)				
1-3	기부금관리 (답례품 판매자)				
2-1	답례품관리 (답례품 주문자)				
2-2	답례품관리 (답례품 수령자)				

6. 개인정보 흐름도

○ 개인정보 흐름도는 개인정보 처리가 수반되는 단위 업무별로 개인정보의 수집, 보유, 이용·제공, 파기 등 개인정보 생명 주기에서의 흐름과 개인정보 우려 사항을 쉽게 파악할 수 있도록 작성함

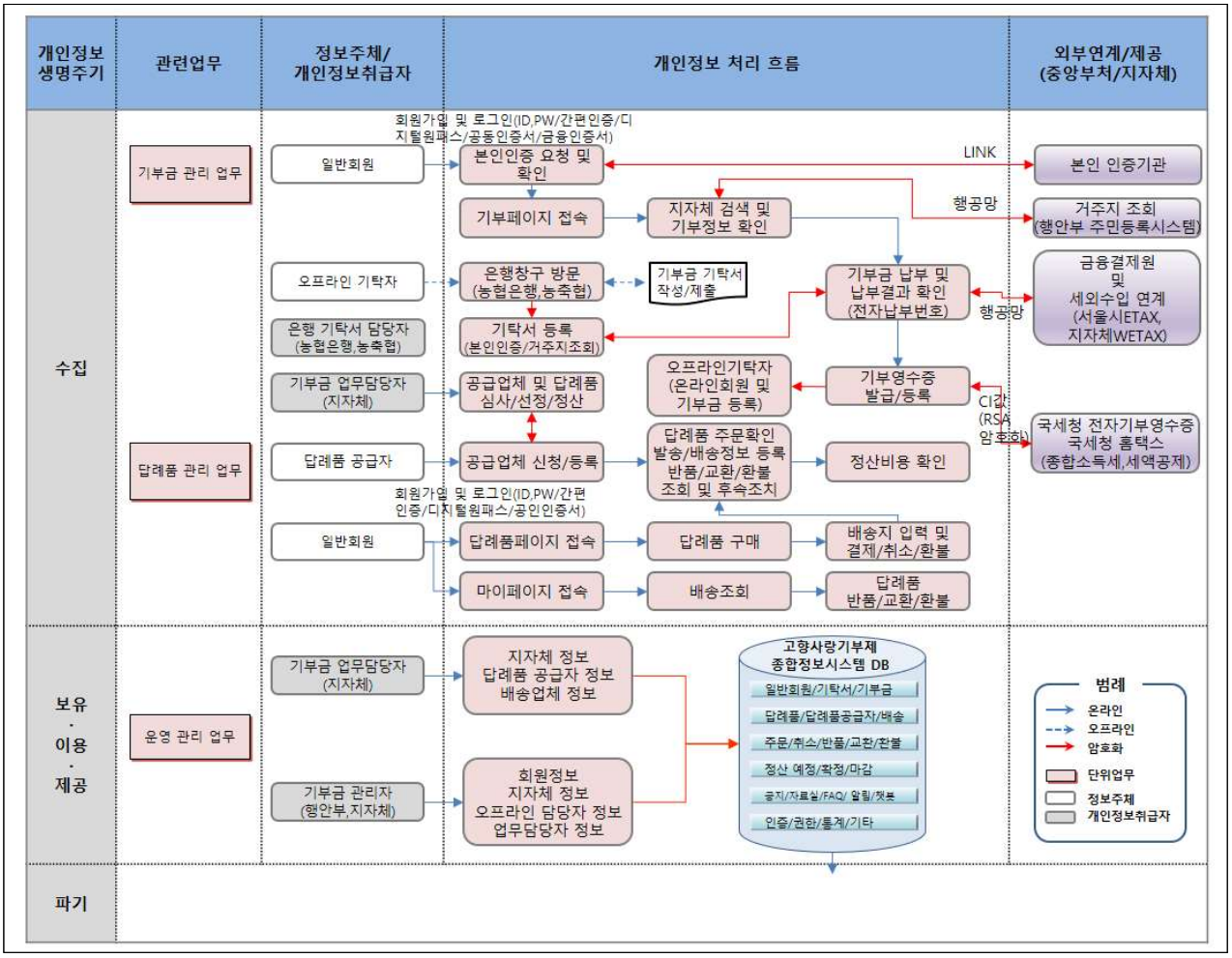
○ 개인정보 흐름도에서 사용된 기호들의 범례는 다음과 같음.

사용기호	설명
정보주체	• 정보주체는 흰색 바탕 도형으로 표기
개인정보취급자	• 개인정보취급자는 회색 바탕 도형으로 표기
정보주체 처리수단	• 정보주체가 처리하는 수단은 좌측 도형과 같이 흰색 바탕으로 표기
개인정보 취급자 처리수단	• 개인정보취급자가 처리하는 수단은 좌측 도형과 같이 밝은 주황 바탕으로 표기
오프라인 온 라 인	• 개인정보의 오프라인 흐름은 점선으로 표기하며, 화살표 방향으로 정보의 흐름이 이동함 • 개인정보의 온라인 흐름은 실선으로 표기하며, 화살표 방향으로 정보의 흐름이 이동함 • 화살표 위에 간략한 업무 설명을 기입함
암호화 구간	• 암호화된 개인정보의 흐름은 붉은색으로 굵게 표기하며, 암호화 개인정보를 붉은색으로 기입
서류보관함	• 오프라인으로 수집된 개인정보파일(신청서 등)은 점선 표기
시스템명 DB 명	• 온라인으로 수집된 개인정보파일은 실선으로 표기하고, 관련 DB명을 표기 • 암호화 항목이 있는 경우 암호화된 항목을 부가로 표기
업무명	• 개인정보 처리업무는 직사각형으로 표기
연계/제공 기관명 (관련 시스템명)	• 연계되는 기관과 해당 시스템은 각각 좌측 도형과 같이 연계·제공 기관명(시스템명)으로 표기
A	• 개인정보 침해요인이 발생하는 부분을 표시하고, 우려 사항에 표기된 번호로 설명
추가설명	• 업무 흐름에 대한 추가 설명

6.1. 총괄 개인정보 흐름도

○ 행정안전부 고향사랑 기부제 종합정보시스템의 총괄 개인정보 흐름도는 아래와 같음

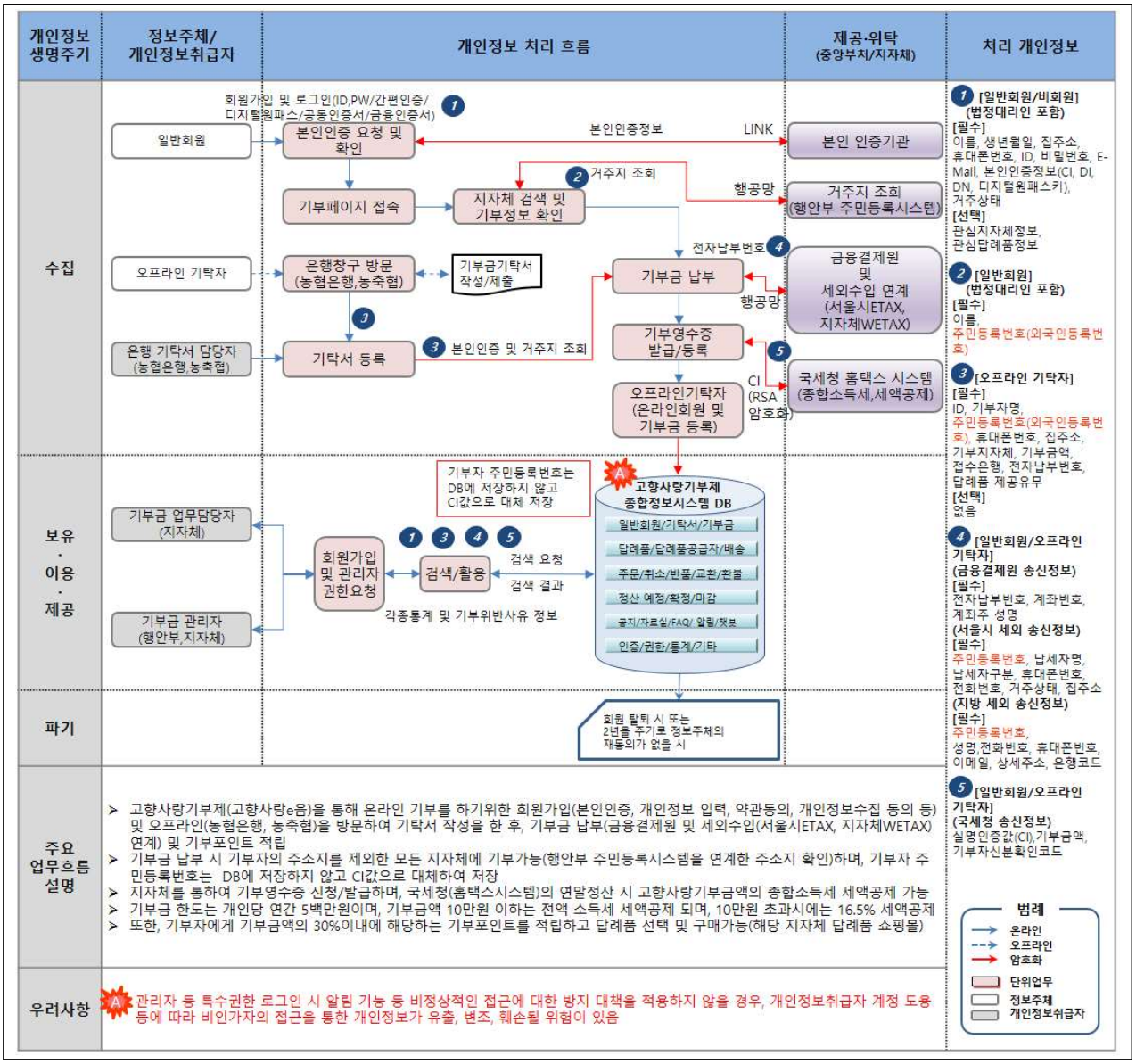
[도표 III-6.1] 고향사랑 기부제 종합정보시스템 총괄 개인정보 흐름도



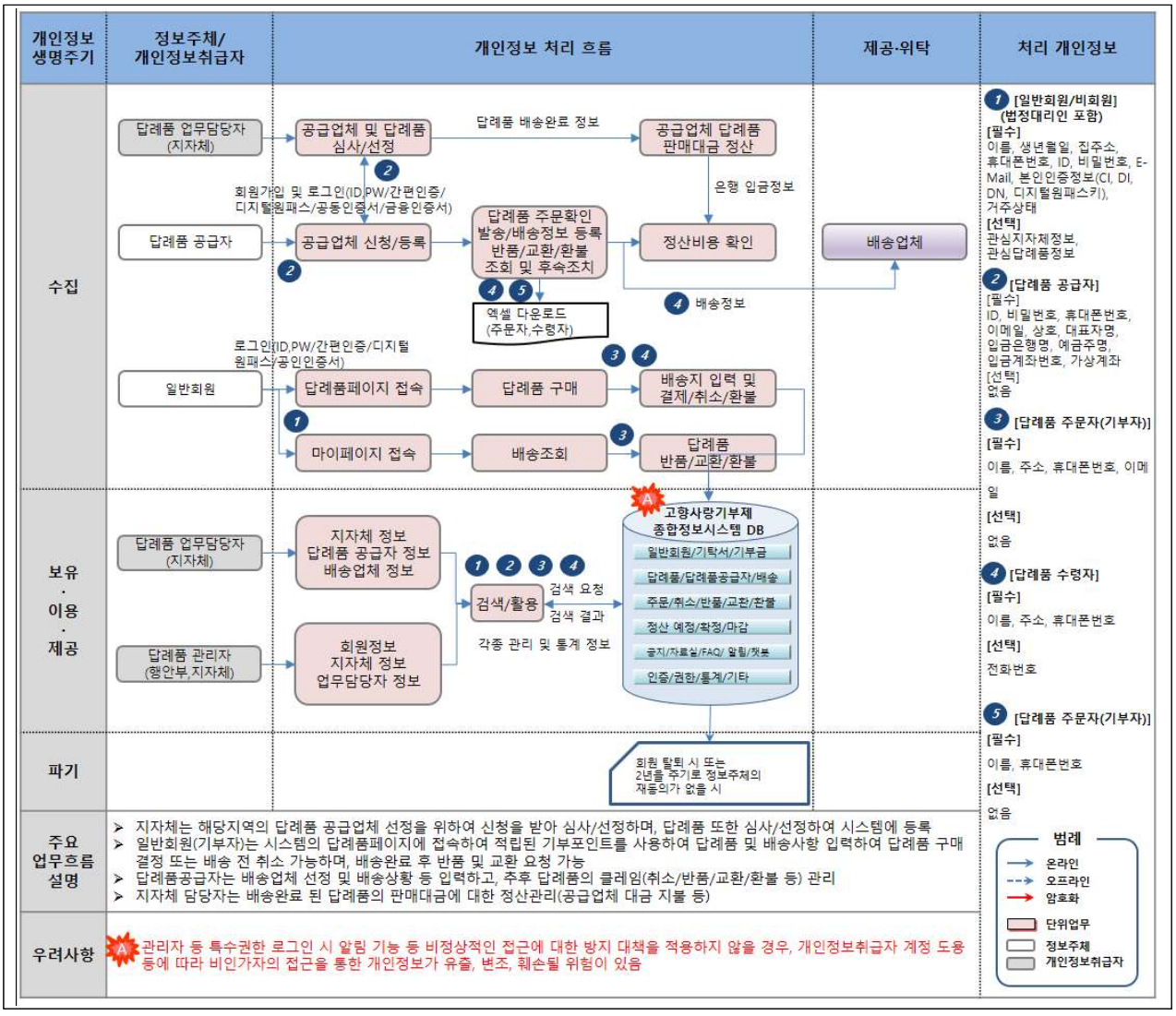
6.2. 상세 개인정보 흐름도

○ 행정안전부 고향사랑 기부제 종합정보시스템의 상세 개인정보 흐름도는 아래와 같음

[도표 III-6.2] 상세 개인정보 흐름도(기부금 관리 업무)



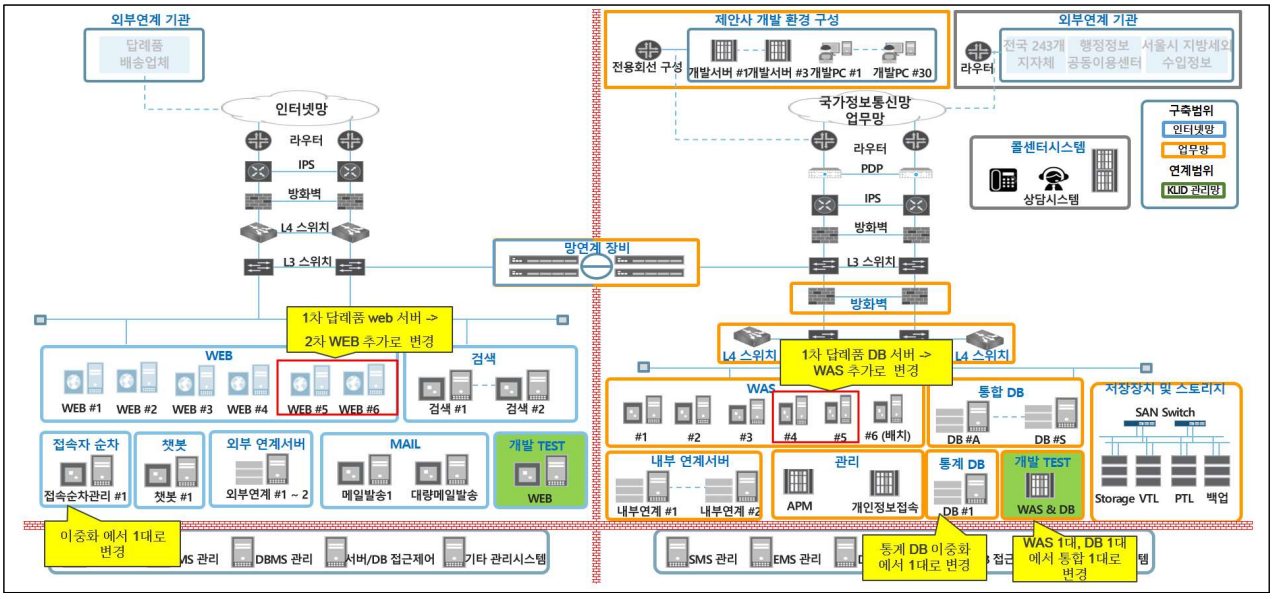
[도표 III-6.3] 상세 개인정보 흐름도(답례품 관리 업무)



7. 시스템 구성도

○ 행정안전부 고향사랑 기부제 종합정보시스템 구성도는 아래와 같음

[도표 III-7.1] 시스템 구성도



8. 정보보호 시스템 목록

○ 행정안전부 고향사랑 기부제 종합정보시스템 관리 시 적용하고 있는 정보보호 시스템 목록은 아래와 같음

[도표 III-8.1] 정보보호 시스템 목록

유형	솔루션 명	목적 및 용도	제조사	비고
방화벽	TrusGuard5000B	외부로부터 내부망을 보호하기 위한 장비로서 외부의 불법 침입으로부터 내부의 정보 자산을 보호하고 외부로부터 유해 정보 유입을 차단하기 위한 장비	㈜안랩	신규 도입
망연계	i-oneNetV5.0	보호 대상의 네트워크를 분리하여, 인가되지 않은 네트워크 차단 및 연결 설정. 네트워크 간 정보보호 제품	㈜휴네시온	신규 도입
서버 접근제어	HI-TAM v5.0	접근제어시스템의 정책에 따라 인가되지 않은 사용자를 접속 차단하기 위한 장비	넷앤드	기 운영중
DB 접근제어	DB-I v6.0	DB 계정 관리, 접근통제, 개인정보 접속기록 저장 등	소만사	기 운영중
ESM	Zenius-EMS v7.0_네트워크 관리	통합 보안 관리시스템 분석	브레인즈컴퍼니	기 운영중
매체제어	nProtect	USB 등 보조 저장매체 제어	㈜잉카인터넷	기 운영중
PC 보안	내PC지키미	PC 취약점 점검 및 조치 솔루션	ZeinSoft	기 운영중
개인정보 유출 차단	셜록홈즈	PC 개인정보보호 솔루션	컴트루테크놀로지	기 운영중
네트워크 접근제어 시스템	Genian NAC	유무선 네트워크 접근제어	지니언스	기 운영중

IV. 개인정보 영향평가 결과

1. 영향평가 항목점검 결과

1.1. 평가영역별 평가 결과

○ 행정안전부 고향사랑 기부제 종합정보시스템에 대한 점검결과, 총 60개 평가항목 중 이행 54개, 부분이행 1개, 미이행 0개, 해당없음 5개로 평가되었으며, 해당없음을 제외한 55개 항목의 이행률은 99%로 확인되었음

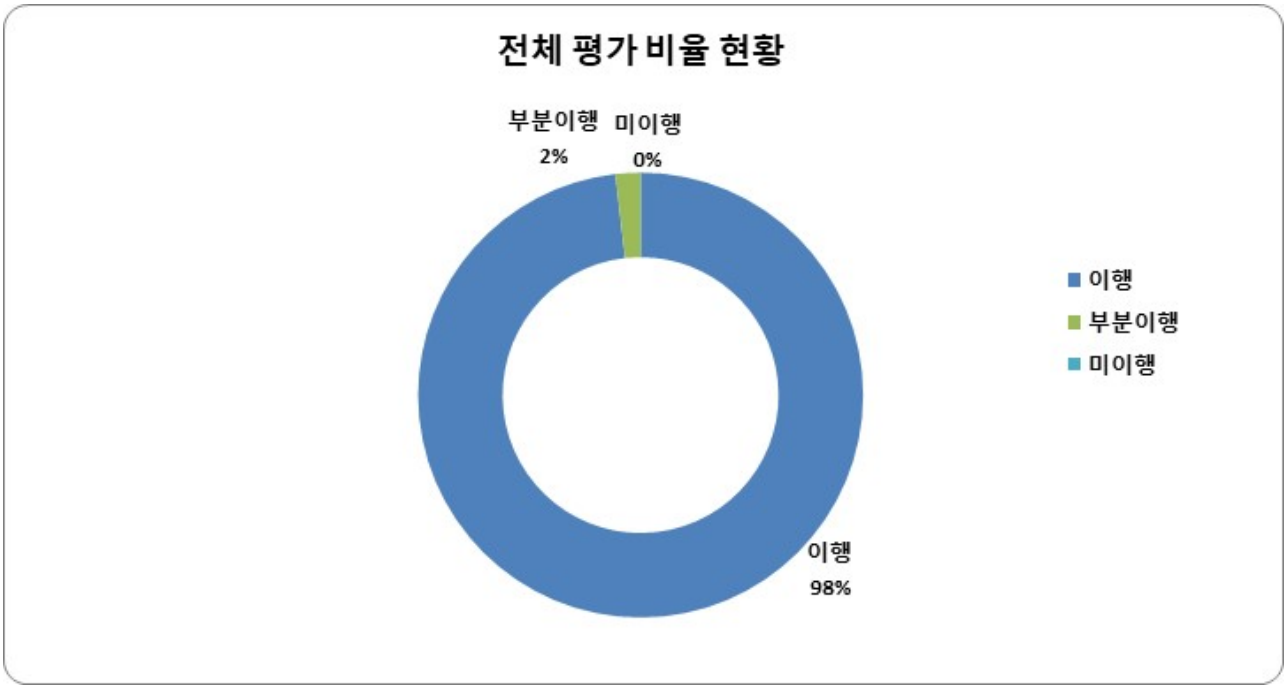
※ 이행률 = (54+1*0.5)/(54+1+0) x 100% = 99%

[도표 IV-1.1] 고향사랑 기부제 종합정보시스템 평가영역별 평가 결과

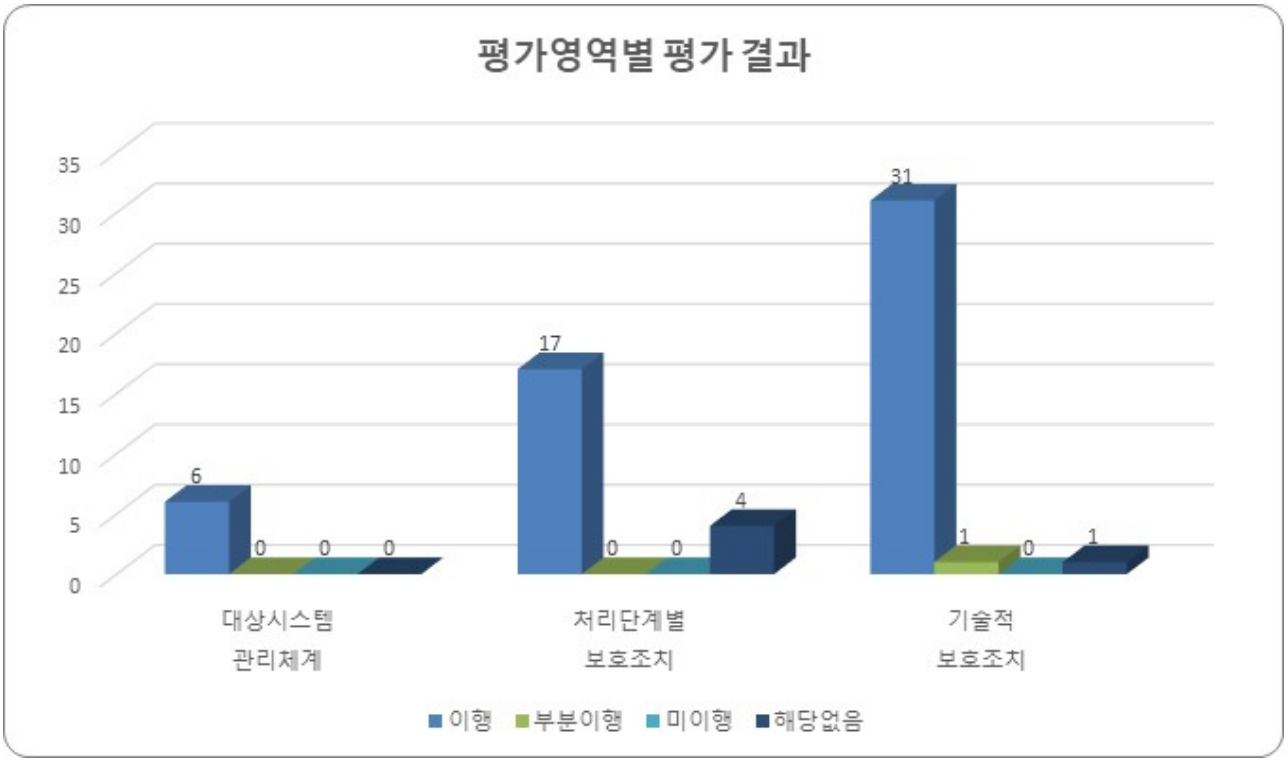
평가결과 / 평가분야	고향사랑 기부제 종합정보시스템				합계	이행률
	이행	부분이행	미이행	해당없음		
1. 대상기관 개인정보 보호 관리체계	-	-	-	-	-	-
2. 대상시스템 개인정보 보호 관리체계	6	0	0	0	6	100%
3. 개인정보 처리단계별 보호	17	0	0	4	21	100%
4. 대상시스템의 기술적 보호조치	31	1	0	1	33	98%
5. 특정 IT기술 활용 시 개인정보보호	-	-	-	-	-	-
합 계	**54**	**1**	**0**	**5**	**60**	**99%**

※ 이행률 = (이행 + 부분이행 X 0.5) / (이행 + 부분이행 + 미이행) X 100

[도표 IV-1.2] 전체 평가 비율 현황(그래프)



[도표 IV-1.4] 평가영역별 평가 결과(그래프)



○ 대상기관의 개인정보보호 관리체계 영역은 개인정보 영향평가를 수행한 후 1년이 지나지 않았으므로 본 평가에서 제외하였음

○ 대상시스템의 개인정보보호 관리체계 영역은 개인정보취급자 관리, 개인정보파일 관리, 개인정보처리방침 등 전반적으로 양호한 상태로 평가함

○ 개인정보 처리단계별 보호조치 영역은 수집, 보유·저장, 이용·제공, 위탁, 파기 등 전반적으로 양호한 상태로 평가함

○ 대상시스템의 기술적 보호조치 영역은 접근통제, 개인정보의 암호화, 접속기록의 보관 및 점검, 악성프로그램 등 방지, 물리적 접근 방지, 개인정보의 파기, 기타 기술적 보호조치, 개인정보 처리구역 보호 등 전반적으로 양호하나 접근권한의 관리 영역에서 일부 미흡한 사항이 발견됨

○ 특정 IT 기술 활용 시 개인정보보호 영역은 대상시스템과 연관성이 없어 평가에서 제외하였음

1.2. 평가 분야별 이행 수준

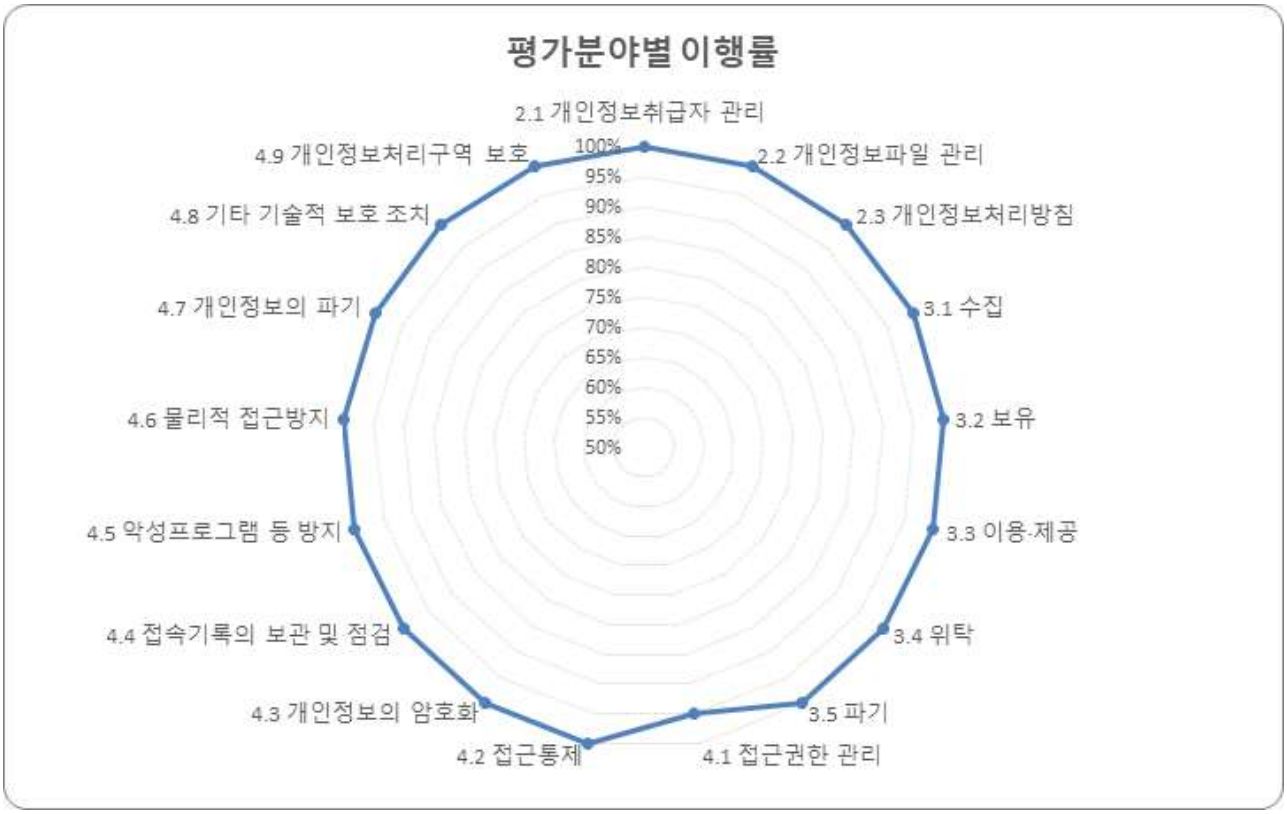
○ 행정안전부 고향사랑 기부제 종합정보시스템의 평가 분야별 이행 수준은 아래와 같음

[도표 IV-1.6] 고향사랑 기부제 종합정보시스템 평가 분야별 이행 수준

평가분야	평가분야(전체)	점검 개수	점검 결과				
			Y	P	N	N/A	이행률
1. 대상기관 개인정보 보호 관리체계	1.1 개인정보보호 조직	-	-	-	-	-	-
	1.2 개인정보보호 계획	-	-	-	-	-	-
	1.3 개인정보 침해대응	-	-	-	-	-	-
	1.4 정보주체 권리보장	-	-	-	-	-	-
2. 대상시스템 개인정보 보호 관리체계	2.1 개인정보취급자 관리	2	2	0	0	0	100%
	2.2 개인정보파일 관리	2	2	0	0	0	100%
	2.3 개인정보 처리방침	2	2	0	0	0	100%
3. 개인정보 처리단계별 보호	3.1 수집	7	7	0	0	0	100%
	3.2 보유	1	1	0	0	0	100%
	3.3 이용·제공	7	3	0	0	4	100%
	3.4 위탁	3	3	0	0	0	100%
	3.5 파기	3	3	0	0	0	100%
4. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	10	9	1	0	0	95%
	4.2 접근통제	6	5	0	0	1	100%
	4.3 개인정보의 암호화	3	3	0	0	0	100%
	4.4 접속기록의 보관 및 점검	3	3	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	3	3	0	0	0	100%
	4.9 개인정보처리구역 보호	3	3	0	0	0	100%
5. 특정 IT기술 활용 시 개인정보보호	5.1 CCTV	-	-	-	-	-	-
	5.2 RFID	-	-	-	-	-	-
	5.3 생체인식정보	-	-	-	-	-	-
	5.4 위치정보	-	-	-	-	-	-
합 계		**60**	**54**	**1**	**0**	**5**	**99%**

※ 범례 [Y(이행), P(부분이행), N(미이행), N/A(해당없음)]

[도표 IV-1.7] 평가 분야별 평가 결과(그래프)



2. 평가영역별 결과

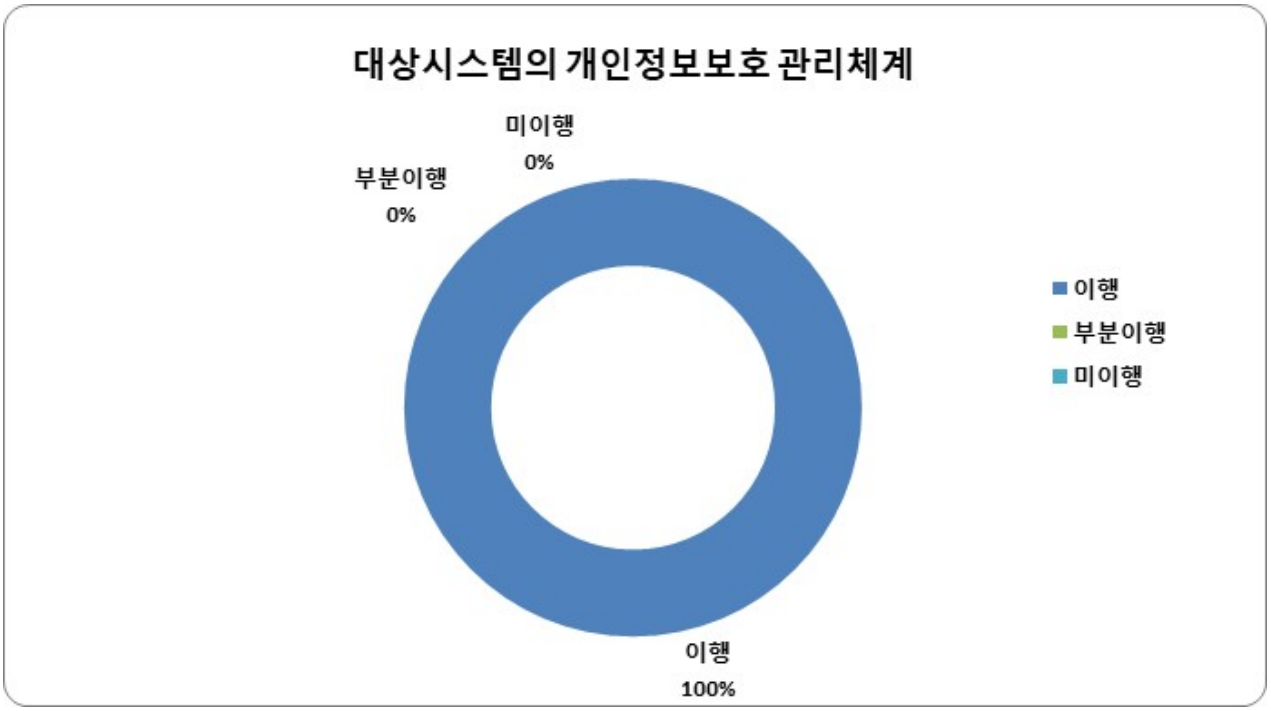
2.1. 대상기관의 개인정보보호 관리체계

○ 1장 대상기관의 개인정보보호 관리체계 영역은 개인정보영향평가를 수행한 후 1년이 지나지 않았으므로 본 평가에서 제외하였음

2.2. 대상시스템의 개인정보보호 관리체계

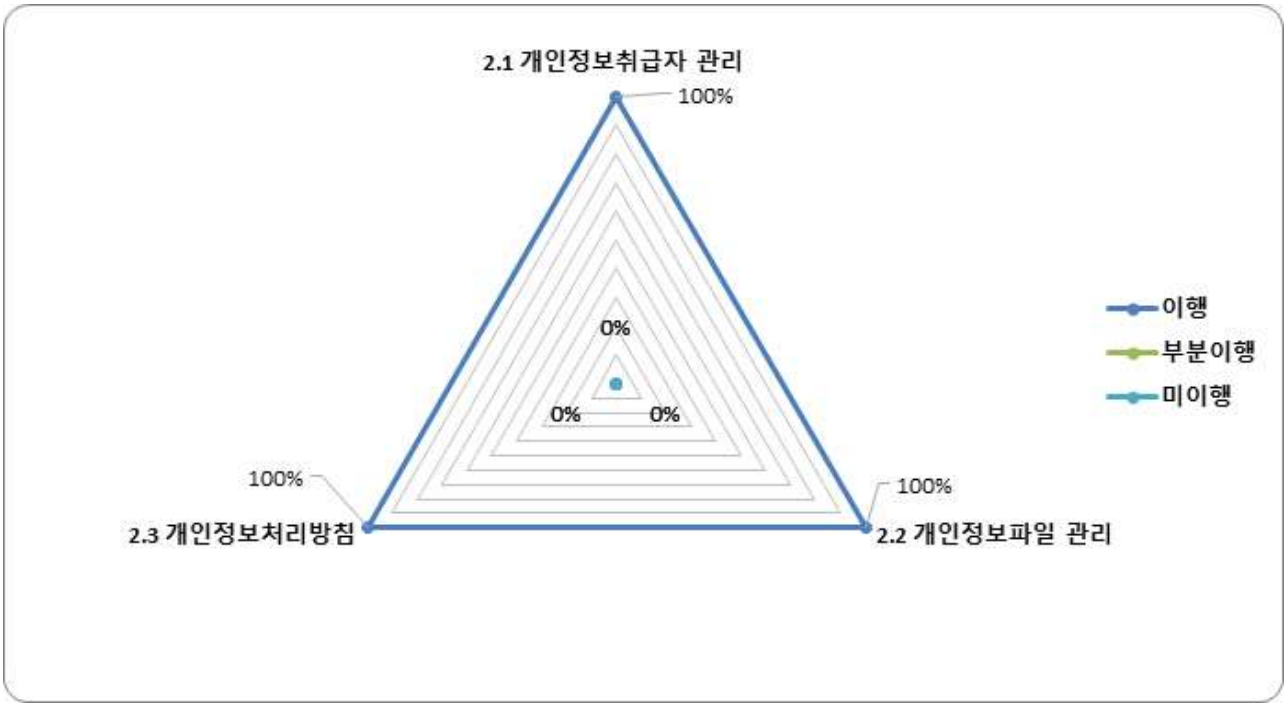
○ 2장 대상시스템의 개인정보보호 관리체계에서는 총 6개 항목 중 이행 6건으로 이행률은 100%로 확인되었음.

[도표 IV-2.4] 대상시스템의 개인정보보호 관리체계 평가 결과



평가영역	이행	부분이행	미이행	해당없음	합계
대상시스템의 개인정보보호 관리체계	6	0	0	0	6

[도표 IV-2.5] 대상시스템의 개인정보보호 관리체계 평가 분야별 결과



평가결과 / 평가분야	대상시스템의 개인정보보호 관리체계				점검 개수	이행률
	이행	부분이행	미이행	해당없음		
2.1 개인정보취급자 관리	2	0	0	0	2	100 %
2.2 개인정보파일 관리	2	0	0	0	2	100 %
2.3 개인정보처리방침	2	0	0	0	2	100 %
합 계	**6**	**0**	**0**	**0**	**6**	**100 %**
평가 비율	**100 %**	**0 %**	**0 %**			

※ 이행률 = (이행 + 부분이행 X 0.5) / (이행 + 부분이행 + 미이행) X 100

[도표 IV-2.6] 대상시스템의 개인정보보호 관리체계 평가 점검표

평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
2. 대상 시스템의 개인 정보 보호 관리 체계	2.1. 개인 정보 취급 자 관리	개인정보 취급자 지정	2.1.1	업무상 필요한 최소한의 범위로 최소한의 인원이 개인정보를 처리하도록 개인정보취급자를 지정하도록 계획하고 있습니까?	●			
		개인정보 취급자 관리·감독	2.1.2	개인정보취급자를 대상으로 역할 및 책임 부여, 개인정보보호 교육, 개인정보보호서약서 작성 등 관리·감독을 계획하고 있습니까?	●			
	2.2 개인 정보 파일 관리	개인정보 파일 대장 관리	2.2.1	대상시스템에서 개인정보파일을 신규로 보유하거나 변경하는 경우, 개인정보파일대장을 작성하거나 변경하도록 계획하고 있습니까?	●			
		개인정보 파일 등록	2.2.2	대상시스템에서 개인정보파일을 신규로 보유하거나 기존파일을 변경하는 경우, 개인정보보호위원회에 등록하도록 계획하고 있습니까?	●			
	2.3 개인 정보 처리 방침	개인정보 처리방침의 공개	2.3.1	개인정보 처리방침을 수립하고 인터넷 홈페이지·관보 등에 안내하도록 계획하고 있습니까?	●			
		개인정보 처리방침의 작성	2.3.2	개인정보 처리방침은 법률 등에서 규정된 내용을 모두 반영하도록 계획하고 있습니까?	●			

(Y : 이행, P : 부분이행, N : 미이행, N/A : 해당없음)

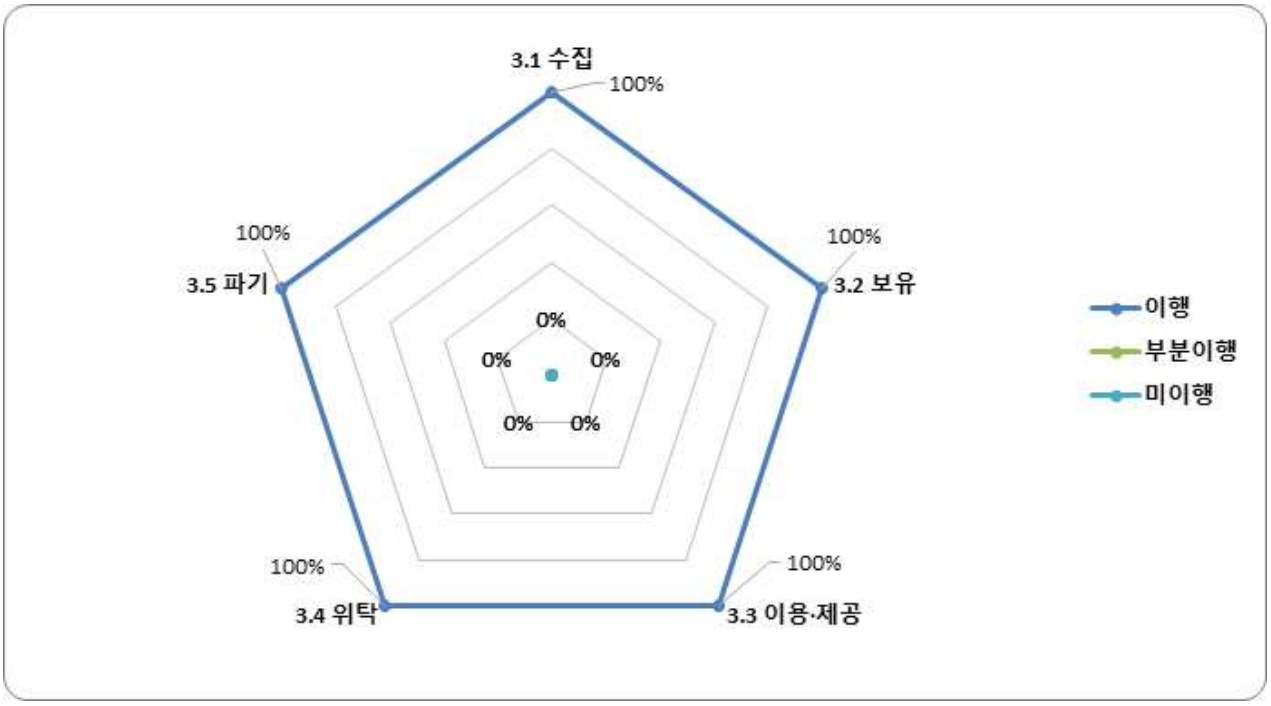
2.3. 개인정보 처리단계별 보호조치

○ 3장 개인정보 처리단계별 보호조치에서는 총 21개 항목 중 해당없음으로 평가된 4개의 항목을 제외한 17개 항목 중 이행 17개, 부분이행 0개로 평가되어 이행률은 100%로 확인되었음

[도표 IV-2.7] 개인정보 처리단계별 보호조치 평가 결과

평가영역	이행	부분이행	미이행	해당없음	합계
개인정보 처리단계별 보호조치	17	0	0	4	21

[도표 IV-2.8] 개인정보 처리단계별 보호조치 평가 분야별 결과



평가결과 / 평가분야	개인정보 처리단계별 보호조치				점검 개수	이행률
	이행	부분이행	미이행	해당없음		
3.1 수집	7	0	0	0	7	100%
3.2 보유	1	0	0	0	1	100%
3.3 이용·제공	3	0	0	4	7	100%
3.4 위탁	3	0	0	0	3	100%
3.5 파기	3	0	0	0	3	100%
합 계	**17**	**0**	**0**	**4**	**21**	**100%**
평가 비율	**100 %**	**0 %**	**0 %**			

※ 이행률 = (이행 + 부분이행 X 0.5) / (이행 + 부분이행 + 미이행) X 100

[도표 IV-2.9] 개인정보 처리단계별 보호조치 평가 점검표

평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
3. 개인정보 처리단계별 보호조치	3.1 수집	개인정보 수집의 적합성	3.1.1	개인정보를 수집하는 경우 법률에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?	●			
			3.1.2	개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고 있습니까?	●			
			3.1.3	주민등록번호는 법적 근거가 있는 경우에 한하여 수집하고 있으며, 인터넷 홈페이지에 대해서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고 있습니까?	●			
		동의받는 방법의 적절성	3.1.4	개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있습니까?	●			
			3.1.5	만14세 미만 아동의 개인정보를 수집하는 경우 법정대리인의 동의를 받도록 계획하고 있습니까?	●			
			3.1.6	개인정보 관련 동의를 서면으로 받을 때에는 중요한 내용을 명확히 표시하여 알아보기 쉽게 하고 개인정보 수집·이용, 제3자 제공, 목적외 이용 등에 대해 각각 구분하여 동의를 받도록 계획하고 있습니까?	●			
			3.1.7	민감정보, 고유식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의를 받도록 계획하고 있습니까?	●			
	3.2 보유	보유기간 산정	3.2.1	개인정보의 보유기간을 법령 기준 및 보유목적에 부합된 최소한의 기간으로 산정하도록 계획하고 있습니까?	●			

평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
	3.3. 이용·제공	개인정보 제공의 적합성	3.3.1	개인정보를 제3자에게 제공하는 경우 법률에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?	●			
			3.3.2	개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 항목으로 제한하도록 계획하고 있습니까?	●			
		목적 외 이용·제공 제한	3.3.3	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 별도의 동의를 받거나 관련 법률에 근거하도록 계획하고 있습니까?				●
			3.3.4	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 이용목적에 맞는 최소한의 항목으로 제한하도록 계획하고 있습니까?				●
			3.3.5	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 '개인정보 목적 외 이용 및 제3자 제공 대장'에 기록·관리하도록 계획하고 있습니까?				●
			3.3.6	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 관련 내용을 관보 또는 인터넷 홈페이지 등을 통해 공개하도록 계획하고 있습니까?				●
		제공시 안전성 확보	3.3.7	개인정보를 제3자(목적 외 제공, 위탁 포함)에게 제공하거나 연계하는 경우 암호화 조치, 보유기간 지정 등 안전성 확보를 위해 필요한 조치를 적용하도록 계획하고 있습니까?	●			
	3.4 위탁	위탁사실 공개	3.4.1	개인정보 처리에 관한 업무 위탁시 위탁하는 업무의 내용, 수탁자 등의 사항을 정보주체에게 공개 또는 통지하도록 계획하고 있습니까?	●			

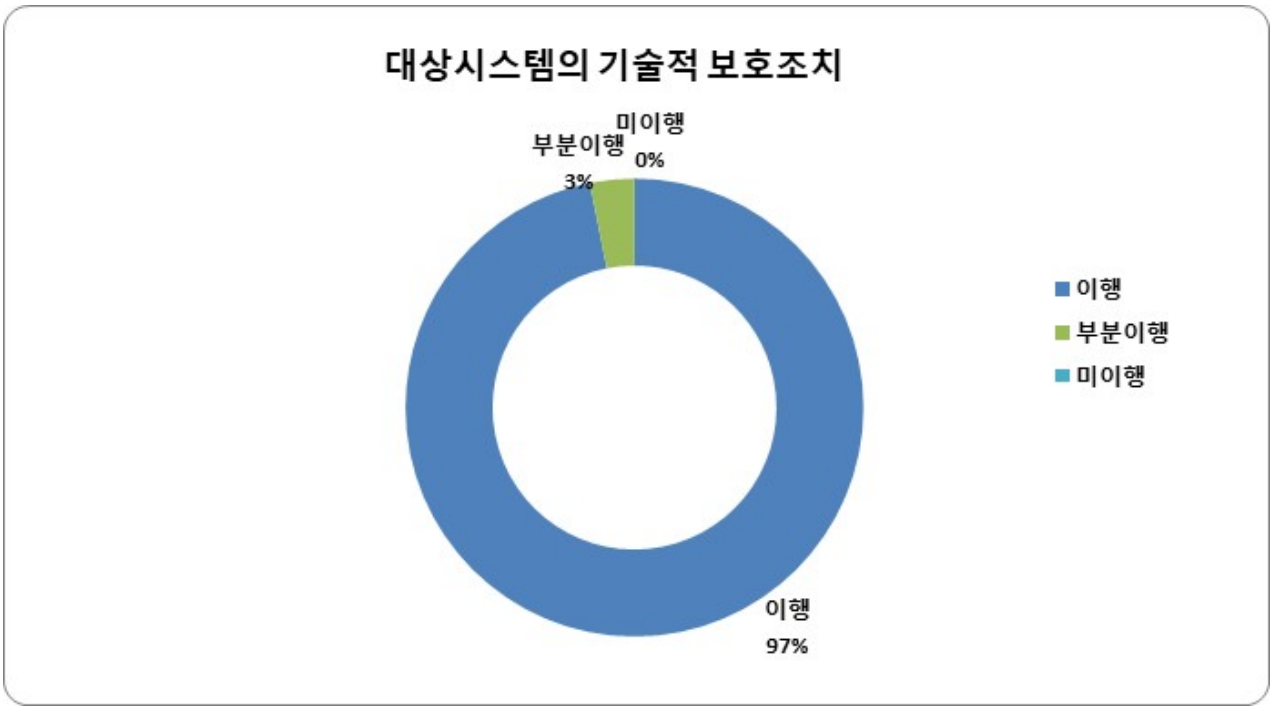
평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
		위탁 계약	3.4.2	개인정보 처리에 관한 업무 위탁 시 개인정보 관리에 관한 책임사항 등이 포함된 문서를 작성하도록 계획하고 있습니까?	●			
		수탁사 관리·감독	3.4.3	개인정보 처리에 관한 업무를 위탁받아 처리하는 자(수탁자)를 대상으로 개인정보보호 교육, 처리현황 점검 등 관리·감독 활동을 계획하고 있습니까?	●			
	3.5 파기	파기 계획 수립	3.5.1	개인정보의 보유 목적이 달성되었거나 보유기간이 경과되었을 때 지체없이 파기되도록 계획하고 있습니까?	●			
		분리보관 계획 수립	3.5.2	다른 법령 등에 따라 개인정보를 보존할 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하도록 계획하고 있습니까?	●			
		파기대장 작성	3.5.3	개인정보파일을 파기하는 경우 파기 결과 등을 '개인정보파일 파기 관리대장'에 기록·관리하도록 계획하고 있습니까?	●			

(Y : 이행, P : 부분이행, N : 미이행, N/A : 해당없음)

2.4. 대상시스템의 기술적 보호조치

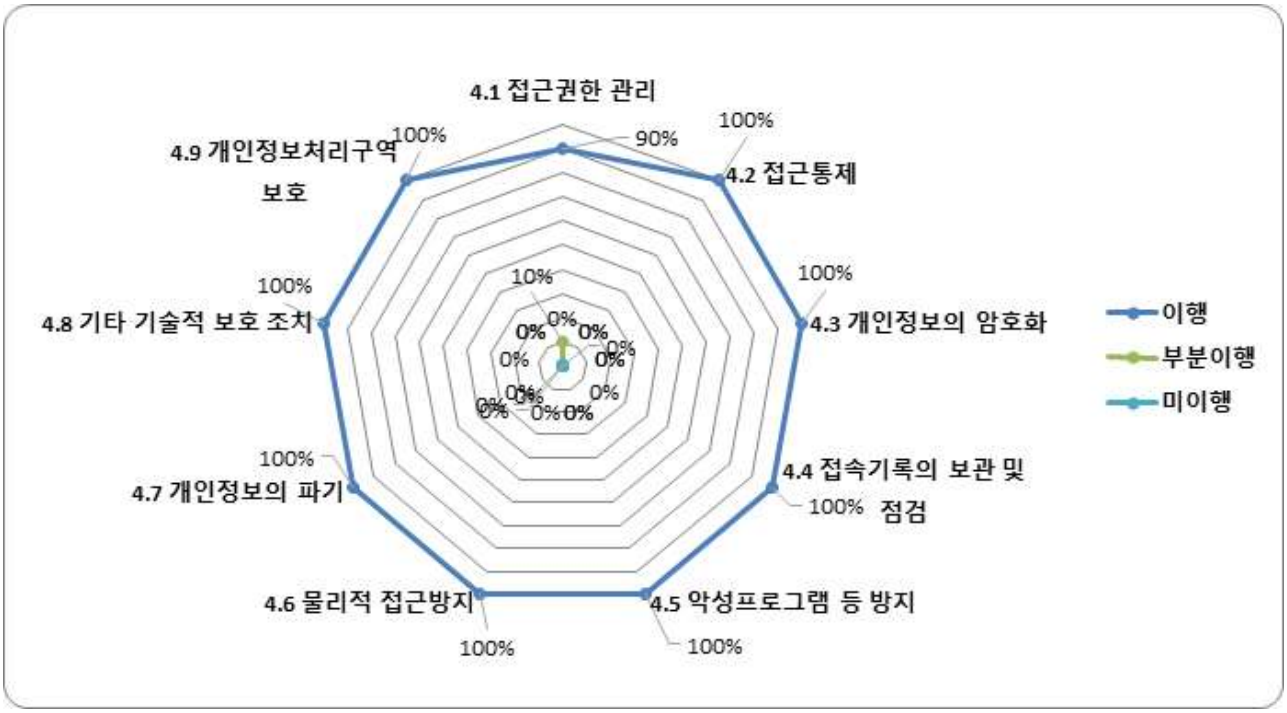
○ 4장 대상시스템의 기술적 보호조치에서는 총 33개 항목 중 해당없음 1건을 제외한 32개 항목에서 이행 31건, 부분이행 1건으로 이행률은 98%로 확인되었음.

[도표 IV-2.10] 대상시스템의 기술적 보호조치 평가 결과



평가영역	이행	부분이행	미이행	해당없음	합계
대상시스템의 기술적 보호조치	31	1	0	1	33

[도표 IV-2.11] 대상시스템의 기술적 보호조치 평가 분야별 결과



평가결과 / 평가분야	대상시스템의 기술적 보호조치				점검 개수	이행률
	이행	부분이행	미이행	해당없음		
4.1 접근권한 관리	9	1	0	0	10	95%
4.2 접근통제	5	0	0	1	6	100%
4.3 개인정보의 암호화	3	0	0	0	3	100%
4.4 접속기록의 보관 및 점검	3	0	0	0	3	100%
4.5 악성프로그램 등 방지	2	0	0	0	2	100%
4.6 물리적 접근방지	2	0	0	0	2	100%
4.7 개인정보의 파기	1	0	0	0	1	100%
4.8 기타 기술적 보호조치	3	0	0	0	3	100%
4.9 개인정보처리구역 보호조치	3	0	0	0	3	100%
합 계	**31**	**1**	**0**	**1**	**33**	**98%**
평가 비율	**97 %**	**3 %**	**0 %**			

※ 이행률 = (이행 + 부분이행 X 0.5) / (이행 + 부분이행 + 미이행) X 100

[도표 IV-2.12] 대상시스템의 기술적 보호조치 평가 점검표

평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
4. 대상 시스템의 기술적 보호조치	4.1 접근 권한 관리	계정 관리	4.1.1	개인정보취급자별로 책임추적성이 확보될 수 있도록 개별 계정을 부여하도록 계획하고 있습니까?	●			
		인증관리	4.1.2	개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 적용하도록 계획하고 있습니까?	●			
			4.1.3	정보주체가 비밀번호 변경 등 중요 정보 접근 시 비밀번호 재확인 등 추가적인 인증이 적용되도록 계획하고 있습니까?	●			
			4.1.4	대량의 개인정보 또는 중요한 개인정보를 처리하는 개인정보취급자 및 관리자는 강화된 인증방식이 적용되도록 계획하고 있습니까?	●			
			4.1.5	개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하고 있습니까?	●			
			4.1.6	개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 계획하고 있습니까?	●			
			4.1.7	개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 장기 미접속시 계정 잠금, 동시 접속 제한, 관리자 로그인 알림 등 보호 대책이 적용되도록 계획하고 있습니까?		●		
		권한 관리	4.1.8	개인정보취급자가 변경될 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하도록 계획하고 있습니까?	●			
			4.1.9	개인정보처리시스템의 접근권한을 부여, 변경 또는 말소한 내역을 기록하도록 계획하고 있습니까?	●			

평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
			4.1.10	개인정보처리시스템에 대한 개인정보취급자의 권한을 조회, 입력, 변경, 삭제, 출력, 다운로드 등 그 역할에 따라 최소한으로 부여할 수 있도록 계획하고 있습니까?	●			
	4.2 접근 통제	접근통제 조치	4.2.1	개인정보처리시스템에 대한 불법적인 접근 및 침해사고를 방지할 수 있도록 접근통제시스템을 설치·운영하도록 계획하고 있습니까?	●			
			4.2.2	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하도록 계획하고 있습니까?	●			
			4.2.3	인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 개인정보가 노출되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자 PC, 모바일기기 등에 보호조치를 계획하고 있습니까?	●			
			4.2.4	개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대한 안전 조치를 적용하도록 계획하고 있습니까?	●			
		인터넷 홈페이지 보호조치	4.2.5	인터넷 홈페이지 취약점으로 인한 개인정보의 유출, 변조, 훼손 등을 방지하기 위하여 웹서버 및 응용프로그램에 대한 취약점점검 및 대응조치를 수행하도록 계획하고 있습니까?	●			
		업무용 모바일기기 보호조치	4.2.6	개인정보를 처리하는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일기기에 비밀번호 설정 등의 보호조치를 계획하고 있습니까?				●
	4.3 개인 정보 의 암호 화	저장시 암호화	4.3.1	고유식별정보, 생체인식정보, 비밀번호 등 중요 개인정보를 저장하는 경우, 안전한 방식으로 암호화 저장하도록 계획하고 있습니까?	●			
			4.3.2	암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하도록 계획하고 있습니까?	●			

평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
		전송시 암호화	4.3.3	고유식별정보, 생체인식정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하도록 계획하고 있습니까?	●			
	4.4 접속기록의 보관 및 점검	접속기록 보관	4.4.1 (변경)	개인정보처리시스템의 접속기록을 개인정보 취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등 필요한 사항이 모두 기록되도록 계획하고 있습니까?	●			
		접속기록 점검	4.4.2 (변경)	개인정보의 유출・변조・훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 정기적(월 1회 이상)으로 점검하고 있으며, 접속기록 점검 시 다운로드한 것이 발견된 경우 내부관리계획으로 정하는 바에 따라 반드시 그 사유를 확인하도록 계획하고 있습니까?	●			
		접속기록 보관 및 백업	4.4.3 (변경)	개인정보처리시스템의 접속한 기록을 최소 1년(5만명 이상의 개인정보를 처리하거나 고유식별정보 또는 민감정보 처리 시 2년) 이상 보관하고 위변조 및 도난, 분실되지 않도록 별도 저장장치 등에 백업 보관하도록 계획하고 있습니까?	●			
	4.5 악성프로그램 등 방지	백신 설치 및 운영	4.5.1	개인정보처리단말기에 악성프로그램을 점검, 치료할 수 있는 백신프로그램을 설치하고 최신업데이트 및 악성프로그램의 주기적 점검 등 대응조치를 실시하도록 계획하고 있습니까?	●			
		보안업데이트 적용	4.5.2	악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램, 운영체제 소프트웨어 제작업체에서 보안 업데이트 공지가 있는 경우, 이에 따른 업데이트가 지체없이 실시되도록 계획하고 있습니까?	●			
	4.6 물리적 접근	출입통제 절차 수립	4.6.1	전산실, 자료보관실 등 개인정보를 보관하는 물리적 장소에 대한 출입통제 절차를 수립·운영하도록 계획하고 있습니까?	●			

평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
	방지	반출·입 통제절차 수립	4.6.2	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고, 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하도록 계획하고 있습니까?	●			
	4.7 개인정보의 파기	안전한 파기	4.7.1	개인정보를 파기할 경우 복구 또는 재생되지 않는 방법으로 파기하도록 계획하고 있습니까?	●			
	4.8 기타 기술적 보호조치	개발환경 통제	4.8.1	개발환경을 통한 개인정보의 유출을 방지하기 위하여 테스트 데이터 생성, 이용, 파기 및 기술적 보호조치 등에 관한 대책을 적용하도록 계획하고 있습니까?	●			
		개인정보 처리화면 보안	4.8.2	개인정보취급자 및 정보주체의 개인정보 처리화면을 통한 개인정보 유·노출 등을 방지하기 위하여 개인정보 마스킹, 웹브라우저 우측 마우스 버튼 제한, 임시 파일 및 캐시 통제, 카드번호 등 중요 정보에 대한 복사·화면캡쳐 방지 및 키보드해킹 방지 등 보호대책을 적용하도록 계획하고 있습니까?	●			
		출력 시 보호조치	4.8.3	개인정보취급자가 개인정보를 종이로 출력할 경우 출력·복사물에 대하여 출력자·출력일시 표시 등의 보호대책을 적용하도록 계획하고 있습니까?	●			
	4.9 개인정보 처리구역 보호조치	보호구역 지정	4.9.1	개인정보처리시스템 및 개인정보를 보관하고 있는 물리적 장소를 보호구역으로 지정하고 물리·환경적인 위협에 대응할 수 있도록 CCTV, 출입통제 장치, 화재경보기 등 보호설비를 설치·운영하도록 계획하고 있습니까?	●			
			4.9.2	개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기 대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검하도록 계획하고 있습니까?	●			

평가 영역	평가 분야	세부분야	질의문 코드	질의문	평가결과			
					Y	P	N	N/A
			4.9.3	개인정보처리자는 재해・재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하도록 계획하고 있습니까?	●			

(Y : 이행, P : 부분이행, N : 미이행, N/A : 해당없음)

2.5. 특정 IT 기술 활용시 개인정보보호

○ 5장 대상기관의 특정 IT 기술 활용 시 개인정보보호는 평가 대상과 연관이 없어 고향사랑 기부제 종합정보시스템 개인정보 영향평가에서는 제외함

3. 침해요인 도출

○ 개인정보 영향평가 평가항목별 점검 결과를 기반으로 침해요인을 도출한 결과, 2장 대상시스템의 개인정보보호 관리체계 0개, 3장 개인정보 처리단계별 보호조치 0개, 4장 대상시스템의 기술적 보호조치 1개 등 총 1개의 침해요인이 도출되었음

3.1. 대상기관 개인정보보호 관리체계

○ 대상 기관 개인정보보호 관리체계 영역은 개인정보영향평가를 수행한 후 1년이 지나지 않았으므로 본 평가에서 제외하였음

3.2. 대상시스템의 개인정보보호 관리체계

○ 침해요인 없음

3.3. 개인정보 처리단계별 보호조치

○ 침해요인 없음

3.4. 대상시스템의 기술적 보호조치

1) 접근권한 관리 분야 현황 및 침해요인 도출

○ (4.1.7) 행정안전부는 서버, DB에서 관리자 등 특수권한 로그인 시 알림 기능을 적용하고 있지 않음

개인정보 침해위험
관리자 등 특수권한 로그인 시 알림 기능 등 비정상적인 접근에 대한 방지 대책을 적용하지 않을 경우, 개인정보취급자 계정 도용 등에 따라 비인가자의 접근을 통한 개인정보가 유출, 변조, 훼손될 위험이 있음

준거성	법적처벌
'개인정보 안전조치 의무'를 위한 권장사항 **'준수미흡'**	'개인정보 안전조치 의무'를 위한 권장사항

3.5. 특정 IT 기술 활용 시 개인정보보호

○ 5장 대상기관의 특정 IT 기술 활용 시 개인정보보호는 평가 대상과 연관이 없어 고향사랑 기부제 종합정보시스템 개인정보 영향평가에서는 제외함

V. 위험평가

1. 위험평가 개요

1.1. 위험평가 목적

○ 영향평가 결과에서 도출된 침해위험을 기준으로 위험평가를 수행하고, 평가 결과에 따라 효과적인 보호 대책 수립을 목적으로 함

1.2. 위험평가 활용

○ 영향평가 결과에서 도출된 침해요인들은 개선하여야 하며, 개선사항의 우선순위를 선정하는데 위험도 산정을 활용할 수 있음

1.3. 위험도 산정 공식

○ 영향평가 수행안내서에는 개인정보 침해위험 요소의 위험도 산정 공식을 아래와 같이 제시하고 있으며, 본 사업에서는 해당 공식을 적용함

[도표 V-1.1] 위험도 산정 공식

위험도 = 자산 가치(영향도) + (침해요인 발생가능성 X 법적준거성) X 2

○ 개인정보 처리가 발생하는 업무와 해당 업무를 통해 처리되는 개인정보의 현황과 각 개인정보 항목의 조합 수준에 따른 영향도를 아래 표와 같이 구분하여 평가함

[도표 V-1.2] 개인정보 영향도(자산 가치) 부여 기준

등급	조합설명	위험성	자산 가치	분류	개인정보 종류
1 등급	그 자체로 개인의 식별이 가능하거나 매우 민감한 개인정보 또는 관련 법령에 따라	- 정보주체의 경제적/사회적 손실을 야기하거나, 사생활을 현저하게 침해 - 범죄에 직접적으로	5	고유 식별정보	주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 ※ 개인정보보호법 제24조 및 동법 시행령 제19조

등급	조합설명	위험성	자산가치	분류	개인정보 종류
	처리가 엄격하게 제한된 개인정보	악용 가능 - 유출 시 민/형사상 법적 책임 부여가능 및 대외 신인도 크게 저하		민감정보	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 병력(病歷), 신체적・정신적 장애, 성적(性的) 취향, 유전자 검사정보, 범죄경력정보 등 사생활을 현저하게 침해할 수 있는 정보 ※ 개인정보보호법 제23조 및 동법 시행령 제18조
				인증정보	비밀번호, 생체인식정보(지문, 홍채, 정맥 등) ※ 개인정보의 안전성 확보조치 기준 고시 제2조
				신용정보 / 금융정보	신용정보, 신용카드번호, 계좌번호 등 ※ 신용정보의 이용 및 보호에 관한 법률 제2조, 제19조 및 동법 시행령 제2조, 제16조, 제21조, 별표2 등 ※ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조제4항제2호 및 관련 고시(개인정보의 기술적·관리적 보호조치 기준) 제6조제2항
				의료정보	건강상태, 진료기록 등 ※ 의료법 제22조, 제23조 및 동법 시행규칙 제14조 등
				위치정보	개인 위치정보 등 ※ 위치정보의 보호 및 이용 등에 관한 법률 제2조, 제16조 등
				기타 중요정보	해당 사업의 특성에 따라 별도 정의
2 등급	조합되면 명확히 개인의 식별이 가능한 개인정보	- 정보주체의 신분과 신상정보에 대한 확인 또는 추정 가능 - 광범위한 분야에서 불법적인 이용 가능 - 유출 시 민/형사상 법적책임 부여	3	개인 식별정보	이름, 주소, 전화번호, 핸드폰번호, 이메일주소, 생년월일, 성별 등
				개인 관련정보	학력, 직업, 키, 몸무게, 혼인여부, 가족상황, 취미 등

등급	조합설명	위험성	자산 가치	분류	개인정보 종류
		가능 및 대외신인도 저하		기타 중요정보	해당 사업의 특성에 따라 별도 정의
3 등 급	개인식별 정보와 조합되면 부가적인 정보를 제공하는 간접 개인정보	- 정보주체의 활동 성향 등에 대한 추정 가능 - 제한적인 분야에서 불법적인 이용 가능 - 대외 신인도 다소 저하	1	자동재생 정보	IP정보, MAC주소, 사이트 방문기록, 쿠키(cookie) 등
				가공정보	통계성 정보 등
				제한적 본인식별 정보	회원정보, 사번, 내부용 개인식별정보 등
				기타간접 개인정보	해당 사업의 특성에 따라 별도 정의

※출처 : 개인정보 영향평가 수행 안내서(2018. 04. 행정안전부/KISA)

○ "[도표 V-1.2]개인정보 영향도(자산 가치) 부여 기준"에 따라 구분한 대상시스템에서 처리하는 개인정보의 영향도(자산 가치) 현황은 아래와 같음

[도표 V-1.3] 개인정보 영향도 등급표

평가 업무	등급	자산 가치	분류	개인정보 종류
기부금 관리	1등급	5	고유식별정보	주민등록번호, 외국인등록번호
			인증정보	비밀번호
	2등급	3	개인 식별정보	이름, 집주소, 휴대폰번호, ID, 이메일, 본인인증정보, 납부자번호, 전자납부번호
			개인 관련 정보	생년월일, 거주상태, 성별, 위반사유
	3등급	1	기타 간접 개인정보	관심지자체정보, 관심답례품정보, 기부지자체, 기부금액, 접수은행, 답례품제공유무
답례품 관리	1등급	5	인증정보	비밀번호

평가 업무	등급	자산 가치	분류	개인정보 종류
	2등급	3	개인 식별정보	이름, ID, 휴대폰번호, 주소, 이메일, 예금주명, 입금계좌번호, 가상계좌
	3등급	1	기타 간접 개인정보	상호, 대표자명, 입금은행명, 대표자명

○ 개인정보 침해요인 발생 가능성은 다음의 표와 같이 4가지로 구분하여 평가함

[도표 V-1.4] 침해요인 발생 가능성 평가 기준

구분	침해요인 발생 가능성	중요도
매우 높음	해당 침해요인의 발생 가능성이 높은 경우	3
높음	해당 침해요인의 발생 가능성이 그다지 높지 않은 경우	2
중간	해당 침해요인의 발생 가능성이 희박하다고 판단되는 경우	1
낮음	해당 침해요인의 발생 가능성이 없는 경우	0

○ 법적 준거성은 다음의 표와 같이 2가지로 구분하여 평가함.

[도표 V-1.5] 법적 준거성 평가 기준

구분	법적 준거성	중요도
높음	법적 준수 사항	1.5
낮음	법률 외 요건(권장 사항)	1

1.4. 위험도 등급 기준

○ 도출된 침해요인에 대한 위험도 수준을 3~14등급으로 나누어 위험도 수준을 평가하며, 14등급에 가까울수록 시스템에 미치는 보안 위험이 크다고 할 수 있음

[도표 V-1.6] 위험도 등급 기준

위험	위험등급	등급기준	대응방안	내용
HIGH	14등급	전사 차원의 매우 심각한 수준의 손실이나 해당 업무의 실패 혹은 경쟁적 지위 상실	즉시 ~ 3개월 이내 조치 필요	정보의 유출, 변조, 파괴, 서비스 중지로 업무수행 및 기관 이미지에 매우 심각한 위험
	13등급	전사 차원의 심각한 수준의 손실이나 해당 업무의 실패 혹은 경쟁적 지위 상실		
	12등급	전사 차원의 심각한 수준의 손실이나 해당 업무의 실패 혹은 경쟁적 지위 하락		
	11등급	매우 심각한 손실이나 해당 업무가 어려워 질 수 있는 정도로 업무에 중대한 영향 발생	3개월 ~ 1년 이내 조치 필요	정보의 유출, 변조, 파괴, 서비스 중지로 업무수행과 기관 이미지에 매우 심각한 위험
	10등급	매우 심각한 손실이나 해당 업무가 어려워 질 수 있는 정도로 일정부분 업무에 중대한 영향 발생		
	9등급	매우 심각한 손실이나 해당 업무가 어려워 질 수 있는 정도로 일정부분 업무에 문제 발생		
	8등급	심각한 손실이나 해당 업무가 어려워 질 수 있는 정도로 일정부분 업무에 문제 발생	검토 후 조치계획 수립	업무수행에 중대한 영향은 발생하지 않으나 관리적 조치가 필요한 상태
	7등급	심각한 손실이나 해당 업무에 부정적인 영향을 줄 수 있는 정도의 문제 발생		
	6등급	심각한 손실이나 해당 업무에 부정적인 영향을 줄 수 있는 정도의 일부분 미약한 문제 발생		
	5등급	해당영역 또는 해당서비스에 작은 영향을 줄 수 있을 정도의 일부분 문제 발생	지속적인 모니터링	업무수행에 위험이 발생하나 심각한 영향이 아니며 빠른 시간 내에 복구 가능
	4등급	해당영역 또는 해당서비스에 미진한 영향을 줄 수 있을 정도로 파급효과가 미약함		
LOW	3등급	업무적으로 영향이 거의 없는 정도로 파급효과가 미약함	담당자 검토	위험이 거의 발생하지 않으나 발생 시에도 업무에 미치는 영향이 미미함

※ 위험 등급별 대응 방안 시기는 해당 시스템의 처리업무 성격, 운영조직, 예산, 사업추진 일정 등에 따라 상기 내용과 상이할 수 있음

2. 위험도 산정 결과

○ 도출된 1개의 개인정보 침해 요소들에 대한 법적 준거성, 자산 가치, 발생 가능성 등을 고려하여 위험도를 산정한 결과 9등급 1개로 산출되었음

[도표 V-2.1] 개인정보 침해 요소별 위험도 산정 결과

[도표 V-2.2] 위험도 산정 결과 위험 등급별 위험 건수

위험등급	3	4	5	6	7	8	9	10	11	12	13	14	합계
위험건수	-	-	-	-	-	-	1	-	-	-	-	-	1
백분율(%)	-	-	-	-	-	-	100	-	-	-	-	-	100

2.1. 대상기관 개인정보보호 관리체계 위험평가 결과

○ 대상 기관 개인정보보호 관리체계 영역은 개인정보 영향평가를 수행한 후 1년이 지나지 않았으므로 본 평가에서 제외하였음

2.2. 대상시스템의 개인정보보호 관리체계 위험평가 결과

○ 해당없음

2.3. 개인정보 처리단계별 보호조치 위험평가 결과

○ 해당없음

2.4. 대상시스템의 기술적 보호조치 위험평가 결과

[도표 V-2.4] 대상시스템의 기술적 보호조치 위험도 산정 내역 - 1

<table>
<tr><td rowspan="2">자산명</td><td>행정안전부 고향사랑 기부제 종합정보시스템</td><td rowspan="2">위험도</td><td rowspan="2">개인정보 영향도</td><td rowspan="2">발생 가능성</td><td rowspan="2">법적 준거성</td></tr>
<tr><td>처리단계</td><td>보유·이용</td></tr>
<tr><td>질의문 코드</td><td>4.1.7</td><td>9</td><td>5</td><td>2</td><td>1</td></tr>
<tr><td>침해요인</td><td colspan="5">관리자 등 특수권한 로그인 시 알림 기능 등 비정상적인 접근에 대한 방지 대책을 적용하지 않을 경우, 개인정보취급자 계정 도용 등에 따라 비인가자의 접근을 통한 개인정보가 유출, 변조, 훼손될 위험이 있음</td></tr>
</table>

2.5. 특정 IT 기술 활용 시 보호조치 위험평가 결과

○ 5장 대상기관의 특정 IT 기술 활용 시 개인정보보호는 평가 대상과 연관이 없어 고향사랑 기부제 종합정보시스템 개인정보 영향평가에서는 제외함

3. 개선방안 도출

○ 개인정보 영향평가 결과에 따라 위험을 도출하고 해당 위험을 제거하기 위한 1개의 개선과제를 다음과 같이 도출하였음

[도표 V-3.1] 고향사랑 기부제 종합정보시스템에서 통제해야 할 위험 및 개선방안

위험도	자산명	질의문 코드	침해요인	개선방안	개선과제
9	고향사랑 기부제 종합정보시스템	4.1.7	관리자 등 특수권한 로그인 시 알림 기능 등 비정상적인 접근에 대한 방지 대책을 적용하지 않을 경우, 개인정보취급자 계정 도용 등에 따라 비인가자의 접근을 통한 개인정보가 유출, 변조, 훼손될 위험이 있음	관리자 등 특수권한 로그인 시 알림 기능 등 개인정보처리시스템에 비정상적인 접근 방지 대책을 마련하여 적용할 것을 권고함	(4.1.7) 비정상적인 접근 방지 기능 구현

4. 개선계획 수립

4.1. 개선계획 목록

○ 개인정보 영향평가 결과 개인정보 침해위험을 제거하기 위한 개선과제 이행이 필요하며, 위험평가 결과에 따라 개선과제의 수행 시기를 제시함.

○ 개선방안을 기준으로 행정안전부 내 보안 조치현황, 예산, 인력, 사업 일정 등을 고려하여 개인정보보호담당자 및 시스템담당자와 협의하여 아래와 같이 개선계획을 수립하였으며, 권장 사항 중 현실적 여건상 적용하기 어려운 과제는 제외하였음

[도표 V-4.1] 개인정보보호 개선계획표

우선순위	개선과제명	개선내용	담당부서	이행구분	수행시기	과제성격
1	비정상적인 접근 방지 기능 구현 (4.1.7)	관리자 등 특수권한 로그인 시 알림 기능 등 개인정보처리시스템에 비정상적인 접근 방지 대책을 마련하여 적용할 것을 권고함	균형발전제도과	권고	장기 (2023.05 ~ 2024.04)	시스템 수정

4.2. 개선계획 상세 이행방안

[도표 V-4.2] 개인정보보호 상세 개선계획 - 1

<table>
<tr><th>우선순위</th><th>1</th><th>관련 평가항목</th><th>4.1.7</th><th>이행구분</th><th>권고</th></tr>
<tr><td>개선과제 명</td><td colspan="5">비정상적인 접근 방지 기능 구현(4.1.7)</td></tr>
<tr><td>법적요건</td><td colspan="5">● 본 항목은 '개인정보 안전조치 의무'를 위한 기술적 보호 방법으로 개인정보의 안전한 보호를 위한 권장 사항임</td></tr>
<tr><td>과제 내용</td><td colspan="5">○ 개인정보처리시스템에 비정상적인 접근에 대한 방지 대책을 적용하지 않을 경우 개인정보취급자 계정 도용 등에 따라 비인가자의 접근을 통한 개인정보가 유출, 변조, 훼손될 위험이 있음

○ 개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위한 보호 대책<예시>은 다음과 같음
1. 업무시간 외 접속 가능 시간제한
2. 일정 기간 미접속 시 계정 잠금
3. 동일 계정에 대한 동시 접속 제한
4. 관리자 등 특수권한 로그인 시 알림 기능
5. 기타 비정상적인 접근을 탐지 또는 방지할 수 있는 보호조치

○ 하지만, 행정안전부의 고향사랑 기부제 종합정보시스템은 한국지역정보개발원의 공통시스템인 서버/DB 접근제어 시스템을 활용하고 있어 서버/DB에 대한 관리자 등 특수권한 로그인 시 알림 기능의 자체적인 적용이 어려움

○ 따라서, 한국지역정보개발원의 공통시스템인 서버/DB 접근제어 시스템에 대하여 관리자 등 특수권한 로그인 시 알림 기능 등 개인정보처리시스템에 대한 비정상적인 접근 방지 대책을 마련하여 적용할 것을 권고함

[비정상적인 접근 방지 기능 구현 방안]
<table>
<tr><th>항목</th><th>개선방안</th></tr>
<tr><td>▪ 관리자 등 특수권한 로그인 시 알림 기능</td><td>▪ 관리자 등 특수권한 계정으로 로그인 시 관리자에게 문자, 이메일, 메신저 등으로 자동 고지함으로써 관리자 계정의 탈취 및 오용 여부를 쉽게 파악할 수 있도록 개선</td></tr>
</table></td></tr>
</table>

	[관리자 로그인 알림 기능 구현(SMS) 예시] 2019-10-29 23:20:39 192.[redacted]1 에서 시스템관리자 님이 로그인하셨습니다.		
수행주체	균형발전제도과	**수행시기**	장기 (2023.05 ~ 2024.04)

(즉시: 1개월 이내, 단기: 3개월 이내, 중기: 6개월 이내 , 장기: 6개월 이상)

VI. 총평

1. 총평

○ 평가항목별로 이행 여부를 점검한 결과,

대상기관의 개인정보 관리체계(1장)는 개인정보 영향평가를 수행한 후 1년이 지나지 않았으므로 본 평가에서 제외함

대상시스템 개인정보보호 관리체계(2장)는 6개 평가항목 중 6개 항목을 모두 적절하게 이행(100%)하고 있음

개인정보 처리단계별 보호조치(3장)는 21개 평가항목 중 해당없음으로 평가된 4개 항목을 제외하고 17개 항목을 모두 적절하게 이행(100%)하고 있음

대상시스템의 기술적 보호조치(4장)는 33개 평가항목 중 해당없음으로 평가된 1개 항목을 제외하고 31개의 항목을 이행(97%) 하고 있으며, 1개 항목에 대해 부분이행(3%)하고 있음

특정 IT 기술 활용 시 개인정보보호(5장) 4개 평가분야 16개 항목은 평가 대상과 연관이 없어 평가에서 제외함

○ 대상기관의 개인정보보호 관리체계 점검 결과,

대상기관의 개인정보보호 관리체계 영역은 22년 10월에 "국가기준데이터 관리체계 구축(5차)" 개인정보 영향평가에서 시행하여 본 영향평가에서는 평가 제외함

○ 대상시스템의 개인정보보호 관리체계 점검 결과,

개인정보취급자 관리, 개인정보파일 관리, 개인정보처리방침 등 대상시스템의 개인정보보호 관리체계가 전반적으로 양호하게 관리되고 있음

○ 개인정보 처리단계별 보호조치에 대한 점검 결과,

개인정보 수집, 보유, 이용·제공, 위탁, 파기 등 개인정보 라이프사이클에 따른 처리단계별 보호조치가 전반적으로 양호하게 관리되고 있음

○ **대상시스템의 기술적 보호조치 점검 결과,**

접근통제, 개인정보의 암호화, 접속기록의 보관 및 점검, 악성프로그램 등 방지, 물리적 접근 방지, 개인정보의 파기, 기타 기술적 보호조치, 개인정보 처리구역 보호 등에 대한 평가 결과는 대체로 양호하게 관리되고 있으나 접근권한 관리 분야의 (4.1.7)에서 미흡한 점이 발견됨

○ **도출된 침해요인은 장기적으로 조치 가능한 사항 1건으로 수행 시기와 개선 계획을 충실히 이행함으로써 조치가 가능할 것으로 판단되므로 개인정보 침해위험을 최소화할 수 있도록 기관 자체적인 노력과 관리가 필요함**

2. 후속 조치

가. 개선이행

- 행정안전부 고향사랑 기부제 종합정보시스템은 영향평가를 시행한 결과 침해요인이 1건 발견되었으므로 제시된 개선방안에 따라 개선할 것을 권고함

나. 영향평가서 제출

- 공공기관의 장은 개인정보보호법 시행령 제35조에 해당하는 개인정보파일을 구축·운용하기 전에 그 영향평가서를 개인정보보호위원회에 제출하여야 함. 다만, 기존에 운용 중이던 개인정보파일인 경우에는 영향평가서를 제출받은 날로부터 2개월 이내에 영향평가서를 개인정보보호위원회에 제출하여야 함
- 개인정보보호 종합포털(intra.privacy.go.kr)의 영향평가 메뉴에서 영향평가서를 등록
  - ✓ 개인정보보호법 제33조(개인정보영향평가)
  - ✓ 개인정보보호법 시행령 제38조(영향평가의 평가 기준 등)
  - ✓ 개인정보 영향평가에 관한 고시 제12조(영향평가서의 제출)

VII. 붙임

1. 개인정보 영향평가 품질검토 체크리스트

1. 개인정보 영향평가 품질검토 체크리스트

○ 수행기관은 영향평가가 충실히 수행되었는지 여부에 대하여 점검하고, 점검 후 미흡한 사항이 있는 경우 보완하기 위하여 아래의 품질검토 체크리스트를 바탕으로 품질검토를 실시하였음

[도표 VII-1.1] 개인정보 영향평가 품질검토 체크리스트

구분	체크리스트		반영 내역
영향평가 보고서 필수사항	1. 영향평가서는 법적 필수사항을 모두 포함하여 작성되었는가? (「개인정보 보호법」 시행령 제38조 제2항)		
	①	개인정보파일 운용과 관련된 사업의 개요 및 개인정보파일 운용의 목적	『영향평가 보고서』 [개인정보 영향평가 보고서 개요] (iv page), I. 추진개요 (1 page)
	②	영향평가 대상 개인정보파일의 개요	『영향평가 보고서』 [개인정보 영향평가 보고서 개요] (iv page), I. 추진개요 (1 page)
	③	평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가 및 개선이 필요한 사항	『영향평가 보고서』 [평가 결과 요약] (vii page), IV. 개인정보 영향평가 결과 (49 page) ~ VI. 총평 (84 page), 『개인정보 영향평가 항목(평가표)』
	④	영향평가 수행인력 및 비용	『영향평가 보고서』 I.6 영향평가 수행인력 및 비용 (17 page)
개인정보 흐름분석의 식별성	2. 평가대상 개인정보파일 및 관련 업무에 대해 총괄 개인정보흐름도 및 업무별 개인정보흐름도가 충실히 작성되었는가?		
	①	[총괄 개인정보흐름도] - 전체 개인정보 흐름을 한눈에 알아볼 수 있도록 작성	『영향평가 보고서』 III.6.1 총괄 개인정보 흐름도 (44 page)
	②	[업무별 개인정보흐름도] - 개인정보 현황분석 단계에서 분류한 개인정보 처리업무 별로 상세한 개인정보 흐름이 파악될 수 있도록 작성 - 평가대상 개인정보파일 및 개인정보 처리업무를 빠짐없이 포함하여 작성	『영향평가 보고서』 III.6.2 상세 개인정보 흐름도 (45 page)

구분	체크리스트		반영 내역
	3. 개인정보흐름도는 개인정보 흐름이 명확히 식별될 수 있도록 구체적으로 작성되었는가?		
	①	- 식별성을 높일 수 있도록 도형, 색상, 기호 등을 활용	『영향평가 보고서』 III.6 개인정보 흐름도 (43 page)
	②	- 우려사항이 있는 경우 흐름도 상에 발생위치를 표시하고 관련 평가항목 번호(지표번호)를 명시하여 평가단계별 추적성 확보	
	③	- 개인정보 수집 방법, 외부 제공 및 연계 방식, 흐름상에 전송되는 정보를 명확히 파악할 수 있도록 작성 등	
평가항목의 적합성	4. 평가항목(평가지표)은 최신 법령·고시 사항이 반영되어 있는가?		
	①	- 개인정보 보호법 및 시행령, 개인정보 처리방법에 관한 고시 - 개인정보의 안전성 확보조치 기준, 표준 개인정보 보호지침 등 관련 고시 ※ 법령, 고시 개정사항은 평가항목에 즉시 반영되어야 하며, 유예기간 등 시행이 확정된 사항에 대해서는 선제적 반영 필요	『영향평가 보고서』 [개인정보 영향평가 보고서 개요] (iv page), I.5.3 평가 기준 (10 page), 『개인정보 영향평가 항목(평가표)』 4.4.1 ~ 4.4.3
	5. 평가항목(평가지표)은 대상 기관 및 시스템의 특성, 최신 보안 위협 등을 반영하여 최적화 되었는가? (해당하는 경우에 한함)		
	①	– 대상 기관이 특별히 적용받는 법령, 고시가 있는 경우, 관련 사항을 평가항목에 반영(의료법, 교육법 등) - 기존 평가항목에 없는 특정 IT기술을 사용하는 경우, 필요한 사항을 평가항목에 추가	보고서 및 평가표에 반영내역 표시
평가항목 점검의 충실성	6. 평가결과에는 오류가 없으며 평가항목별 증적이 객관적이고 상세하게 제시되었는가?		
	①	- 평가증적은 제3자가 보더라도 평가결과를 납득할 수 있도록 구체적으로 제시되어야 함(화면 캡처, 설계문서 사진 등)	『개인정보 영향평가 항목(평가표)』 전체
	②	- 법령, 고시 등 법적 요건에 대한 해석 및 점검에 오류사항이 없어야 함	
	③	- 개인정보 현황 및 흐름도, 대상 기관 및 시스템의 현황과 비교하여 점검 결과에 오류사항이 없어야 함	
	7. 평가항목 점검 결과는 개인정보 흐름분석 단계와 연계성이 확보되었는가?		
	①	- 개인정보 흐름분석 단계에서 식별된 개인정보 수집, 저장, 이용, 제공 및 파기 경로, 외부 위탁 관련 사항이 빠짐없이 점검되어야 함	『개인정보 영향평가 항목(평가표)』 전체

구분	체크리스트		반영 내역
	8. . 평가항목 별로 반드시 점검해야 할 세부점검 사항이 빠짐없이 점검되었는가?		
	①	- 평가항목 별로 반드시 점검되어야 할 세부 점검사항에 대해서는 빠짐없이 점검을 수행하고 점검표에 평가결과를 기록해야 함	『개인정보 영향평가 항목(평가표)』 전체
	9. 기술적 보호조치 관련 영역 점검 시 응용시스템 뿐만 아니라, 평가 범위에 포함된 서버, DBMS 등 인프라 영역에 대한 점검도 수행되었는가? (서버, DBMS 등 인프라 영역이 영향평가 범위에 포함된 경우에 한함)		
	①	- 영향평가 범위에 서버, DBMS 등 인프라 영역이 포함되어 있는지 확인 후, 평가범위에 포함되어 있다면 평가항목별 점검 시 응용시스템 외에 서버, DBMS 영역에 대한 점검도 함께 수행 필요	『개인정보 영향평가 항목(평가표)』 전체
	②	- 표준배포시스템의 경우 중앙에서 수행한 평가지표에 대해서는 제외 가능하지만 서버, DBMS 등을 지자체에서 직접 관리하고 있다면 해당 영역에 대해서는 평가 수행 필요	해당없음
위험분석의 합리성	10. 침해요인의 내용 및 위험도의 크기는 실질적인 위험을 대변할 수 있도록 합리적으로 도출되었는가?		
	①	- 침해요인의 내용은 대상 기관 및 시스템의 관점에서 어떤 문제가 있는지 명확히 알 수 있도록 구체적이고 알기 쉽게 표현되어야 함	보고서 및 평가표에 반영내역 표시
	②	- 법규 위반 관련 침해요인은 어떤 조항을 위반한 것이며 그로 인해 어떤 처벌과 문제가 발생할 수 있는지를 알 수 있도록 기술되어야 함	
	③	- 위험분석 절차는 논리적이고 합리적인 방법론으로 수행되어야 하며, 위험도의 크기는 대상 기관 및 시스템의 관점에서 실질적인 위험의 크기를 대변할 수 있어야 함	
개선 계획의 활용성	11. 침해요인 별로 개선방안이 빠짐없이 제시되었으며, 개선계획은 즉시 활용가능 하도록 구체적이고 실질적인 내용으로 수립되었는가?		보고서 및 평가표에 반영내역 표시
	①	- 도출된 모든 침해요인을 해결할 수 있도록 개선 방안이 빠짐없이 제시되어야 함	
	②	- 각 개선방안은 해당 침해요인을 효과적으로 해결할 수 있는 최적의 방안이 제시되어야 함	
	③	- 평가기관의 일방적 제안은 지양하고, 개선방안 및 개선계획 수립시 실제 이행을 담당할 조직 및 담당자와 충분한 협의를 수행해야 함	
	④	- 개선방안 및 개선계획은 대상기관이 즉시 활용하여 이행할 수 있도록 전문적이고 상세하게 제시되어야 함	

VIII. 별 첨

1. 개인정보 영향평가 항목(평가표)