2021

APEC CBPR 인증

국경 간 개인정보 처리에 관한 인증 안내서



개인정보보호위원회
Personal Information Protection Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

PART I

CBPR 인증 개요

1. CBPR 인증 개요 ····· 8
   1.1. CBPR 인증 개념 및 특징 ····· 8
   1.2 CBPR 인증의 효용 ····· 8
   1.3 CBPR 인증의 개인정보 보호 원칙 ····· 9

2. CBPR 인증 운영체계 및 도입 현황 ····· 10
   2.1 CBPR 인증 운영체계 ····· 10
   2.2 CBPR 인증 가입 및 인증 취득 ····· 11
   2.3 CBPR 인증 가입국 및 인증기업 현황 ····· 13

PART II

CBPR 인증체계

1. CBPR 인증체계 ····· 16

2. CBPR 인증심사 단계별 준비 사항 ····· 17
   2.1 인증심사 준비 ····· 19
   2.2 인증심사 ····· 24
   2.3 인증서 발급 ····· 26
   2.4 인증 유지·관리 ····· 28

PART III

CBPR 인증기준

1. 개인정보 관리 체계 수립 34
1.1 정책 수립 34
1.2 책임자 지정 36

2. 개인정보 수집 38
2.1 최소 수집 38
2.2 개인정보 처리방침 공개 43
2.3 수집 시 고지 46

3. 개인정보 이용/제공/위탁 52
3.1 이용 52
3.2 제공/위탁 55
3.3 자료 제출 요구 대응 59

4. 정보주체 권리 61
4.1 열람권 61
4.2 정정·삭제권 65
4.3 선택권 67
4.4 민원제기 73

5. 무결성 75
5.1 최신성 유지 75
5.2 최신정보 공유 78

6. 보호 대책 80
6.1 보호대책 수립/이행 80
6.2 보호대책 평가/개선 87
6.3 수탁사의 보호대책 88
6.4 제3자의 보호대책 94
6.5 파기 96
6.6 임직원 인식제고 98



APEC CBPR 인증 안내서

국경 간 개인정보 처리에 관한 인증

들어가기

목적

- 본 안내서는 아시아-태평양 경제협력체(Asia-Pacific Economic Cooperation, APEC) 회원국 공동 개인정보 보호 인증체계인 APEC CBPR(Cross Border Privacy Rules) 인증에 대해 상세히 설명하기 위해 마련되었다.
- APEC은 디지털 경제의 활성화를 위해 회원국 간 정보 이동의 장벽 제거와 소비자 정보 프라이버시 보호에 대한 신뢰 확보가 중요함을 인식하여 2005년 APEC 프라이버시 프레임워크(APEC Privacy Framework)를 승인한 바 있다. CBPR은 본 프레임워크 내 프라이버시 보호 원칙을 담은 인증체계로서, 개인정보의 국내 처리뿐만 아니라 국외 이전 처리를 포괄한다.
- 안내서는 APEC의 운영 원칙이나 인증기관의 인증 지침의 변경 등에 따라 지속적으로 수정, 보완될 수 있으므로 본 안내서를 참고할 때는 항상 최신의 버전 여부를 확인한다. 한국인터넷진흥원(KISA)의 CBPR 인증 운영에 관한 자료는 KISA 홈페이지 내 CBPR 인증 안내 페이지에서 확인할 수 있다. 또한 APEC에서 운영하는 CBPR 공식 홈페이지(영문)(cbprs.org)에서는 CBPR 인증 가입국가, 해외 인증기관, 인증 취득 기업 등의 일반 현황에 대한 정보를 확인할 수 있다.

적용 대상

- 국내 개인정보 보호법 적용 대상 기관 또는 기업(이하 기업)은 인증 신청이 가능하며 특히 다음과 같은 기업이 CBPR 인증 효용이 높다.
  - 아시아 태평양 지역을 비롯한 국외에 개인정보를 이전하거나 국외로부터 개인정보를 이전받아 처리하는 또는 처리할 가능성이 있는 기업
  - 아시아 태평양 지역을 비롯한 다수의 국가에 계열사, 자회사 등이 위치하여, 전사에 적용할 통일된 개인정보 보호 지침이 필요한 기업
  - 개인정보 국외 이전 처리는 없으나 향후 사업 계획 등을 고려하여 글로벌 기준의 개인정보 보호 체계를 수립하고자 하는 기업

용어

- CBPR 인증은 APEC 프라이버시 보호 원칙을 기반으로 설계되었으며, 따라서 CBPR의 용어는 이 원칙에서 규정한 것을 따른다. 그러나 국내 기업 등에게는 생소한 일부 표기법이나 용어에 대해서는 이에 대한 이해를 돕기 위해 CBPR 용어를 국내 개인정보 보호법의 대응되는 용어로 대체하여 표기하거나 두 용어를 병기한다.
- CBPR 인증과 비교하여 설명되는 개인정보 보호법에서 제6장 '정보통신서비스 제공자등의 개인정보 처리 등 특례' 규정의 '이용자'와 '정보통신서비스 제공자등'은 각각 동 법 내 일반 규정의 대응 용어인 '정보주체'와 '개인정보처리자'로 통칭하여 표기한다.



APEC CBPR 인증

국경 간 개인정보 처리에 관한 인증 안내서

PART I

CBPR 인증 개요

1. CBPR 인증 개요
2. CBPR 인증 운영체계 및 도입 현황

CBPR 인증 개요

1. CBPR 인증 개요

1.1. CBPR 인증 개념 및 특징

- APEC 프라이버시 보호 원칙을 기반으로 기업의 개인정보 보호 체계를 평가하여 인정하는 글로벌 인증제도로서, APEC 회원국 간 공동의 개인정보 보호 기준을 통해 자유롭게 안전한 개인정보 이전을 지원하고자 APEC 회원국 공동으로 개발했다.

- CBPR 인증은 회원국 또는 기업의 자율적 참여를 기반으로 운영되며, 제도 운영 국가에서 별도의 규정이 있지 않는 한 CBPR 인증을 취득한다고 해서 자국의 법령에서 요구하는 의무를 경감하거나 면제하지 않는다. 그러나 CBPR을 운영하는 국가의 관련 규범이나 법집행 체계를 바탕으로 운영되어 인증에 대한 공신력을 더한다.

1.2. CBPR 인증의 효용

1.2.1 기업의 효용

- 각 국가의 CBPR 인증에 대한 인센티브 정책이나 인증 취득 기업의 수, 그리고 CBPR에 대한 인지도나 신뢰도 형성에 따라 인증의 실질적 효용성에 차이가 있음을 전제한다.

- 먼저, 국가가 CBPR을 자국의 공인 인증제도로 승인하거나 법제화하는 경우 직접적인 법제도적 혜택을 받을 수 있다. 이 경우 CBPR 인증 취득 기업은 공인 개인정보 보호 모범 기업으로 대외

신뢰도를 높일 수 있으며, 법에서 정한 다른 의무 사항이나 제재 등에서 면제·경감되거나 정부 지원 정책 등의 우선 수혜 대상이 될 수 있다.

CBPR을 국가 공인 인증으로 승인한 사례

CBPR 인증 가입국 중 일본, 싱가포르 등은 CBPR을 자국의 개인정보 보호 규범과 동등한 수준의 보호 체계로서 인정하고 이를 법령에 반영하였다. 즉, 개인정보를 국외로 이전할 수 있는 요건에 CBPR 인증을 포함하여, CBPR 인증을 취득한 국외 기업에 정보주체의 동의 획득 등의 절차 없이 개인정보를 이전할 수 있도록 했다. CBPR 제도의 운영은 CBPR 가입국만 가능하나, 이와 같이 CBPR을 인정하는 정책 도입은 CBPR 가입국 외에도 어느 국가도 가능하다. 그 예로 버뮤다 제도도 CBPR을 개인정보 국외 이전 허용 요건으로 인정(2021년)한 바 있다.

- 그 외 일반적 효용으로는, 타 기업과의 업무 제휴, 위탁, 계약 및 해외의 개인정보 처리 시스템 사용 등을 통해 개인정보를 국외에 이전하여 처리하거나 국외로부터 이전받아 처리하는 기업의 경우,
  - CBPR 인증을 통해 상대국 또는 상대 기업에 자사의 개인정보 보호 수준을 입증함으로써 대외 신인도를 높이고,
  - 반대로 CBPR 인증을 취득한 상대 기업에 대해 보호 수준을 확인하는데 필요한 시간과 비용을 줄이고 최소한의 보호 수준을 보장받을 수 있다.
- 또한 글로벌 기업의 경우, 개별 국가의 개인정보 보호 규범에 각각 대응해야 하는 법령 준수 부담 및 비용을 덜고, 글로벌 공동의 인증기준인 CBPR을 전사에 적용하여 통일된 정책을 수립할 수 있다.

1.2.2 정보주체의 효용

- CBPR 인증을 통해, 자신의 정보가 이전되는 기업이 적절한 보호 수준을 갖춘 기업인지 여부를 확인할 수 있다. 또한 CBPR 인증 운영 국가 또는 인증기관 간의 집행 협력 체계를 통해 국외에 이전된 개인정보에 대한 정보주체의 권리 행사나 피해 구제 신청이 편리해진다.

1.3. CBPR의 개인정보 보호 원칙

- APEC은 회원국 간 자유롭고 신뢰할 수 있는 교역을 위해 'APEC 프라이버시 프레임워크(APEC Privacy Framework, APF)'를 개발하여 개인정보 이전 원칙과 체계를 수립하였다(2005년). APF는 고지, 수집 제한, 목적 내 이용, 선택권, 무결성, 보호대책, 열람·정정권, 책임성, 피해 구제 등 9가지 프라이버시 원칙을 담고 있다. CBPR은 개인정보 처리 시 이러한 9원칙을 이행하기 위한 50개의 인증기준(requirements)이다.

APEC 프라이버시 9 원칙

① **고지**	개인정보 처리에 대한 사전 고지
② **수집 제한**	수집 목적과 관련된 정보를 합법적이고 공정하게 수집, 적절한 경우 동의 획득
③ **목적 내 이용**	수집 목적과 양립가능(compatible)하거나 관련(related)된 목적 내 이용
④ **선택권**	적절한 경우 정보주체에게 수집·이용·제공에 대한 처리 제한권 부여
⑤ **무결성**	개인정보의 정확성, 완전성, 최신성 유지
⑥ **보호대책**	피해 발생 가능성과 심각성, 정보의 민감성에 비례한 보호조치 이행
⑦ **열람·정정**	정보주체의 개인정보 열람·정정·삭제권 보장
⑧ **책임성**	CBPR 원칙을 이행할 수 있는 내부 및 수탁사 등에 대한 책임성 있는 관리체계 수립·이행
⑨ **피해 구제**	개인정보 오용 방지를 위한 설계, 피해의 개연성과 심각성에 비례한 피해 구제 조치

2. CBPR 운영체계 및 도입 현황

2.1 CBPR 운영체계

2.1.1. CBPR 운영 조직

- CBPR은 APEC 회원국이 공동으로 개발한 국제 인증제도로서 CBPR 운영에 관한 사항은 APEC에서 주관한다. APEC 내 CBPR 인증 운영 실무 조직을 중심으로 CBPR 운영 가이드라인 및 인증기준 개발, 제도 확산 활동, CBPR 신청 국가 및 인증기관에 대한 심의 등의 업무가 수행되며 최종 의사 결정은 회원국 의견 수렴을 통해 이루어진다.

APEC 내 CBPR 운영 조직

APEC 내 디지털 경제 운영그룹(Digital Economy Steering Group, DESG)의 하부 그룹인 데이터 프라이버시 소그룹(Data Privacy Subgroup, DPS)에서 회원국의 개인정보 보호 관련 이슈를 논의하며, 이 DPS 내 CBPR에 관한 사항을 심의, 감독하는 공동감독위원회(Joint Oversight Panel, JOP)가 있다.

- 그 외 CBPR의 세부 평가 기준, 심사 방법 등 구체적인 제도 운영에 관한 사항은 각 회원국 또는 인증기관에서 정하여 운영할 수 있다.

2.1.2. CBPR 운영체계

- CBPR은 가입국의 개인정보 보호 관련 규범이나 감독기구의 법집행력을 기반으로 하여 운영된다. 즉 CBPR 취득 기업이 형식에 그치지 않고 실제 인증기준을 잘 이행할 수 있도록, CBPR 운영에 적용 가능한 법령 및 법집행 체계가 갖추어진 국가에 한하여 운영할 수 있도록 했다.

CBPR 이행 지원을 위한 관련 국내 법

- 회원국이 CBPR을 운영하기 위해서는 CBPR을 집행할 수 있는 자국의 관련 법령이 있어야 한다. 이 관련 법령은 반드시 개인정보 보호법이여야 하는 것은 아니며, CBPR 인증기준을 이행하도록 작동하는 다른 형태의 규범이 될 수도 있다.
  - 예를 들어, 우리나라는 개인정보 보호 원칙이 명시된 개인정보 보호법이 CBPR의 인증기준을 충족하여 이를 바탕으로 CBPR을 운영한다. 그러나 (개인정보 보호에 대한 연방 법령이 없는) 미국의 경우, 기업의 개인정보 처리에 대한 불공정하고 기만적인 행위를 규율하는 연방거래위원회법(FTC Act)을 기반으로 CBPR을 운영한다. 이 법에 따라 연방거래위원회(FTC)는 CBPR 인증 기업이 이를 이행하지 않을 경우 기만행위로 간주하여 집행이 가능하다. 즉 FTC Act와 FTC는 각각 CBPR 이행의 관련 법령과 법집행 기관으로 승인받았다. 캐나다도 이와 유사한 접근으로 경쟁법(Competition Act) 및 상표법(Trade-Marks Act)을 관련 법령으로 승인 받았다.

2.2 CBPR 가입 및 인증 취득

2.2.1 회원국의 CBPR 가입 및 승인

- CBPR 운영을 위해서는 먼저 국가 차원의 CBPR 가입이 필요하다. 신청국은 자국이 CBPR을 집행할 수 있는 관련 법령 및 법집행 체계 등이 갖추어져 있음을 증명하는 서류 등을 APEC에 제출하여 APEC의 승인을 받아야 한다.
- APEC의 심의를 통해 최종 가입(승인) 여부가 결정되며 이후 인증기관 지정 등의 필요한 단계를 밟을 수 있다. 우리나라는 2017년에 가입 승인된 바 있으며 우리나라의 CBPR 이행의 관련 법령과 법집행 기관은 각각 개인정보 보호법과 개인정보보호위원회이다.

2.2.2 인증기관 신청 및 인정

- APEC으로부터 자격을 인정받은 기관이 CBPR 인증을 수행할 수 있다. CBPR 인증기관이 되기 위해서는 첫째, 인증기관의 인증 활동을 규율*할 수 있는 자국의 관련 법령 및 법집행 기관이 있어야 한다. 둘째, APEC이 마련한 독립성, 인증절차, 집행 매커니즘 등 7가지 인증기관 자격 요건을 충족해야 한다. APEC의 인정을 받기 위해서는 먼저 자국 내 CBPR 법집행 기관 등으로부터 인증기관 후보로 지명 받거나 신청 희망 기관이 자발적으로 신청 서류 제출하여 관할 법집행 기관 등의 검토를 받을 수 있다.

  * 인증기관이 부정하게 인증을 발급하거나 인증 신청자와 부적절한 이해관계를 형성하는 등의 부정행위에 대해 규율할 수 있어야 한다.

- CBPR 인증기관은 민간 또는 공공기관 여부에 상관없이 신청가능하며, 한 국가에 다수의 인증기관이 운영될 수 있다. 우리나라는 한국인터넷진흥원(KISA)이 2019년에 APEC으로부터 인정받았다.

2.2.3 CBPR 인증 신청 범위

- 기업이 CBPR 인증을 취득하려면 원칙적으로 CBPR 신청인이 속한 국가가 CBPR에 가입하여야 하며, 해당 국가의 인증기관을 통해 인증을 받을 수 있다. CBPR에 가입한 국가이나 인증기관이 지정되지 않는 등의 경우에는 다른 나라의 인증기관을 이용할 수도 있는데, 다만 이러한 경우에도 타국의 인증기관의 행위를 규율할 수 있는 자국의 관련 법령 등이 있어야 하며, 이에 대해 APEC의 인정을 받아야 한다.

- 또한 자국에 인증기관이 있다고 하더라도, 모든 기업이 CBPR 인증대상이 되는 것은 아니다. 해당국이 CBPR 가입 시 승인받은 관련 법령의 적용 범위에 대해 인증이 가능하며, 따라서 우리나라의 경우 현재 CBPR 가입 관련 법령인 개인정보 보호법 적용 대상 기업이 인증 신청이 가능하다. APEC의 CBPR 운영 규정에 따라 정부기관은 인증 대상이 아니다.

2.2.4 CBPR 인증기업 공개

- CBPR 인증을 취득한 기업은 KISA 홈페이지 내 CBPR 안내 페이지에 공개되며, 국내외 모든 CBPR 인증 취득 기업에 대한 정보는 APEC의 CBPR 공식 홈페이지(cbprs.org) 통해 확인가능하다. 인증 취득 기업의 기업명, 연락처, 인증 유효 기간을 비롯하여 인증을 발급한 인증기관, 관할 법집행 기관, 국가 등의 정보를 공개해 대중에 기업의 개인정보 보호 수준에 대한 인지도나 책임성을 높인다. 또한 정보주체는 피해 구제를 신청할 수 있는 창구(관련 기관명, 연락처 등)를 확인할 수 있다.

2.3 CBPR 가입국 및 인증기관 현황(2021년 11월 기준)

- 현재 CBPR 가입국은 미국(2012년), 멕시코(2013년), 일본(2014년), 캐나다(2015년), 싱가포르(2018년), 호주(2018년), 대만(2018년), 필리핀(2020년) 등 9개국이다*.

  * 현재 APEC 회원국에 한하여 CBPR 가입을 신청할 수 있으나 향후 CBPR의 효용을 넓히기 위해 회원국 이외 다른 국가까지 확대하는 방안이 꾸준히 논의되고 있다.

- CBPR 인증기관으로는 우리나라의 KISA를 비롯하여 미국의 TrustArc, Schellman, NCC Group, HITRUST, BBB National Programs, 일본의 JIPDEC(일본정보경제사회추진협회), 싱가포르의 IMDA(정보통신미디어개발청), 대만의 III(산업정보연구소) 등 9개 기관이 있으며, 정보보안 또는 개인정보 보호 평가 업체, 사업자 협회, 공공기관 등 다양한 분야의 기관들로 구성되어 있다.



APEC CBPR 인증

국경 간 개인정보 처리에 관한 인증 안내서

PART II

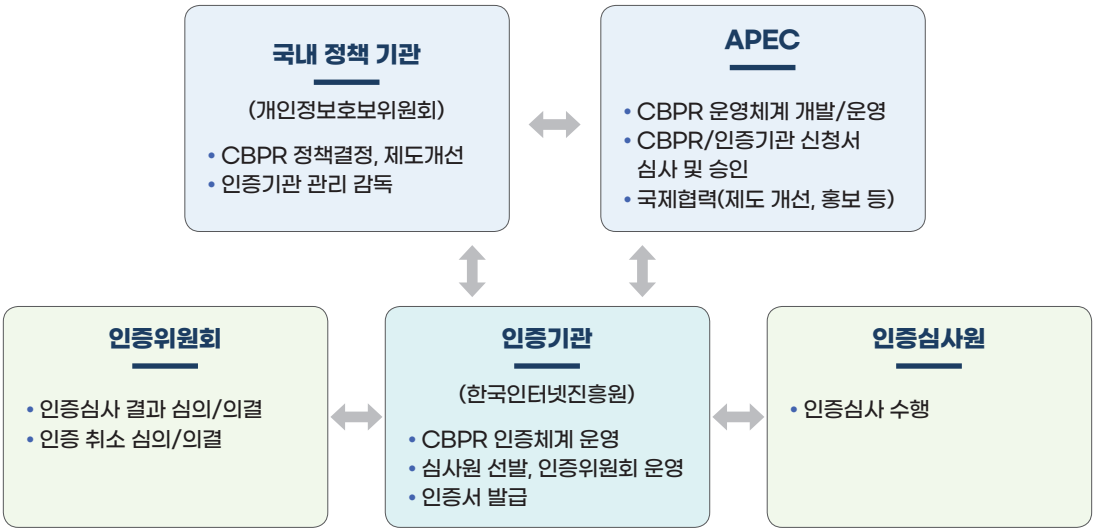
CBPR 인증체계

1. CBPR 인증체계
2. CBPR 인증심사 단계별 준비 사항

II CBPR 인증체계

1. CBPR 인증체계

- 한국인터넷진흥원(KISA)은 APEC의 CBPR 운영 체계를 기반으로 CBPR 인증에 관한 정책 결정, 인증심사, 심사결과 심의, 인증서 발급 및 KISA의 인증 활동에 대한 관리·감독 등의 인증 체계를 수립하였다. KISA 외 각각의 역할을 수행하는 정책기관, 인증심사원, 인증위원회 등으로 구성되었다.



- **(APEC)** CBPR 운영체계를 개발·운영하는 조직으로 CBPR 인증에 참여하려는 국가 또는 인증기관에 대한 심의와 승인한다. 또한 제도 개선, 회원국 내 CBPR 인증 확산 등을 위한 국제협력을 주관한다. (☞ 상세한 내용은 앞장 CBPR 인증 개요 파트 중 2.1 CBPR 운영체계 부분 참조)

- **(국내 정책기관)** CBPR 인증제도 관련 정책 수립, 인증기관 지정(인증기관 최종 승인은 APEC에서 심사·결정) 역할을 하는 기관으로 국내에서는 개인정보보호위원회가 있다. 개인정보보호위원회는 인증기관의 인증활동에 대한 관리·감독 등 인증기관 활동에 대한 집행 권한이 있다.

- **(인증기관)** CBPR 인증체계 수립, 인증심사, 인증서 발급 등 인증 제도를 실무적으로 운영한다. 인증기관인 KISA는 심사팀을 구성하여 신청인이 수립·운영하는 개인정보 관리체계가 CBPR의 인증기준에 적합한지 여부를 심사하고 인증서를 발급한다. 또한 인증위원회 운영, 인증심사원 선발, 인증제도 및 기준 개선 등 CBPR 인증제도 전반에 걸친 업무를 수행한다.

- **(인증위원회)** 인증심사 결과가 적합한지 여부, 인증 취소에 관한 사항, 이의신청에 관한 사항 등을 심의·의결한다. 인증위원회는 개인정보 보호 전문가, 변호사, 교수 등 개인정보 보호 분야에 학식과 경험이 있는 자 중에서 10명 내외의 위원으로 구성되어 운영된다.

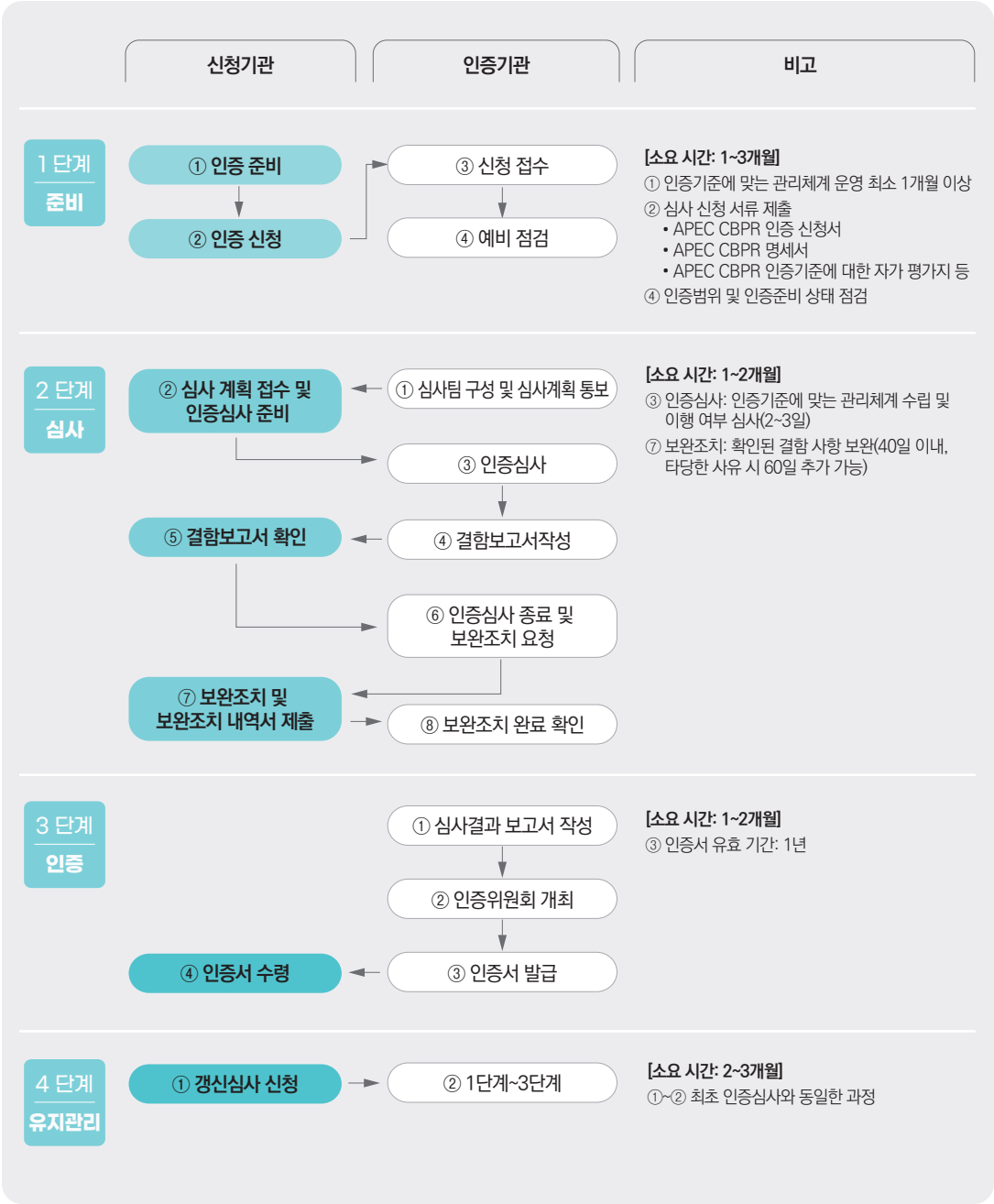
- **(인증심사원)** 인증심사를 수행하는 자로 개인정보 보호, 정보보안 분야 전문가 중 인증기관이 선발한다. 심사를 위해 인증기관 소속의 심사 팀장과 심사원으로 구성된 심사팀을 운영한다.

2. CBPR 인증심사 단계별 준비 사항

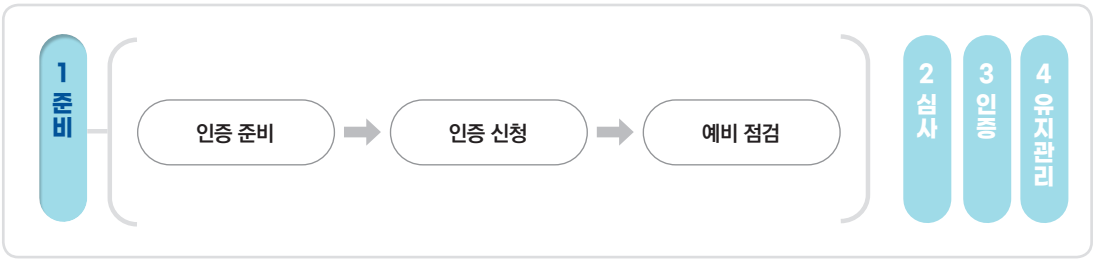
CBPR 인증심사 절차는 다음 그림과 같다. 인증심사 준비 및 신청부터 인증서 발급까지는 인증심사의 범위 등에 따라 차이가 있으며 일반적으로 3개월~5개월 정도가 소요된다. 이에, 인증서 발급을 희망하는 시기가 있다면 5개월 이전에 인증심사 준비를 할 필요가 있다.

CBPR 인증 범위에 대해 ISMS-P 인증을 먼저 취득한 경우 신청인의 심사 준비 기간이 비교적 단축되고, 사안에 따라 심사 기간도 단축될 수 있다.

CBPR 인증심사 절차


신청기관
인증기관
비고
1 단계
준비
① 인증 준비
② 인증 신청
③ 신청 접수
④ 예비 점검
[소요 시간: 1~3개월]
① 인증기준에 맞는 관리체계 운영 최소 1개월 이상
② 심사 신청 서류 제출
• APEC CBPR 인증 신청서
• APEC CBPR 명세서
• APEC CBPR 인증기준에 대한 자가 평가지 등
④ 인증범위 및 인증준비 상태 점검
2 단계
심사
② 심사 계획 접수 및 인증심사 준비
① 심사팀 구성 및 심사계획 통보
③ 인증심사
⑤ 결함보고서 확인
④ 결함보고서작성
⑥ 인증심사 종료 및 보완조치 요청
⑦ 보완조치 및 보완조치 내역서 제출
⑧ 보완조치 완료 확인
[소요 시간: 1~2개월]
③ 인증심사: 인증기준에 맞는 관리체계 수립 및 이행 여부 심사(2~3일)
⑦ 보완조치: 확인된 결함 사항 보완(40일 이내, 타당한 사유 시 60일 추가 가능)
3 단계
인증
① 심사결과 보고서 작성
② 인증위원회 개최
④ 인증서 수령
③ 인증서 발급
[소요 시간: 1~2개월]
③ 인증서 유효 기간: 1년
4 단계
유지관리
① 갱신심사 신청
② 1단계~3단계
[소요 시간: 2~3개월]
①~② 최초 인증심사와 동일한 과정

2.1 인증심사 준비



2.1.1 CBPR 인증 준비

- 신청인은 인증 신청서를 제출하기 전에 CBPR 인증기준에 따라 CBPR 체계를 구축하고 최소 1개월 이상 운영한 증적을 준비해야 한다.
- 신청인은 인증 받고자 하는 인증 범위를 정할 때 개인정보 관련 업무를 상세하게 분석하여 라이프사이클(수집·보유·이용·제공·폐기)에 따른 개인정보 흐름을 고려하여 모든 서비스, 인력 등을 포함하여야 한다.
- CBPR 인증 범위를 정할 때는 이용자 중심의 대외 서비스만 포함할 것인지 임직원이 이용하는 내부 서비스 까지도 포함할 것인지에 대해서도 고려하여야 한다. 특히 해외에 위치한 법인, 제휴사 등에 개인정보를 이전하여 처리할 계획이 있는 경우는 관련 개인정보 처리에 대한 사항이 모두 포함되는지 확인한다.
- 신청인은 CBPR 인증을 받기 위해 CBPR 인증기준에 맞게 자가 진단하고 관련 내용을 검토하여 CBPR 인증기준을 충족하지 못하는 부분에 대해서는 보완 조치를 완료하여야 한다.

자가진단 방법

- CBPR 인증기준에 따라 신청인이 운영 중인 현황 여부를 점검 (O, X 표시)
- 운영사항을 이행사항과 미 이행사항을 기록하고 특히 미 이행사항에 대한 문제점은 상세히 기록
- 문제점에 대한 개선계획(보호대책)을 수립하고 개선방법을 기술하고 일정에 맞게 개선 조치

2.1.2 인증 신청

- 인증심사 신청 시 다음의 서류들을 준비하여 인증 또는 심사기관에 제출한다.

CBPR 인증심사 신청 서류

- APEC CBPR 인증 신청서
- APEC CBPR 명세서
- APEC CBPR 인증기준에 대한 자가 평가지
- APEC CBPR 인증심사에 대한 확약서(서명 후 제출)
- 법인/개인 사업자등록증 또는 고유번호증
- 기타 증빙서류

※ 신청서 및 CBPR 명세서, 자가 평가지 양식 및 CBPR 인증심사에 대한 확약서 양식은 KISA 홈페이지 내 CBPR 안내 웹페이지 참조

- **(신청서)** CBPR 신청서에는 신청인의 기본 정보와 최초/갱신 심사 여부, 인증 범위 등을 기재하여 대표자의 서명 후 제출한다.

APEC CBPR 신청서

※ 색상이 어두운 난은 신청인이 작성하지 아니하며, [ ]에는 해당되는 곳에 √표를 합니다.

접수번호		접수일시	처리기간
신청인	업체명		사업자등록번호
	대표자		전화번호
	주소		
	전자우편(e-mail)		
구분	심사구분	[ ]최초심사	[ ]갱신심사
	※ ISMS-P 획득 여부[ ] - 유효기간( ), 인증범위( )		
	인증범위		

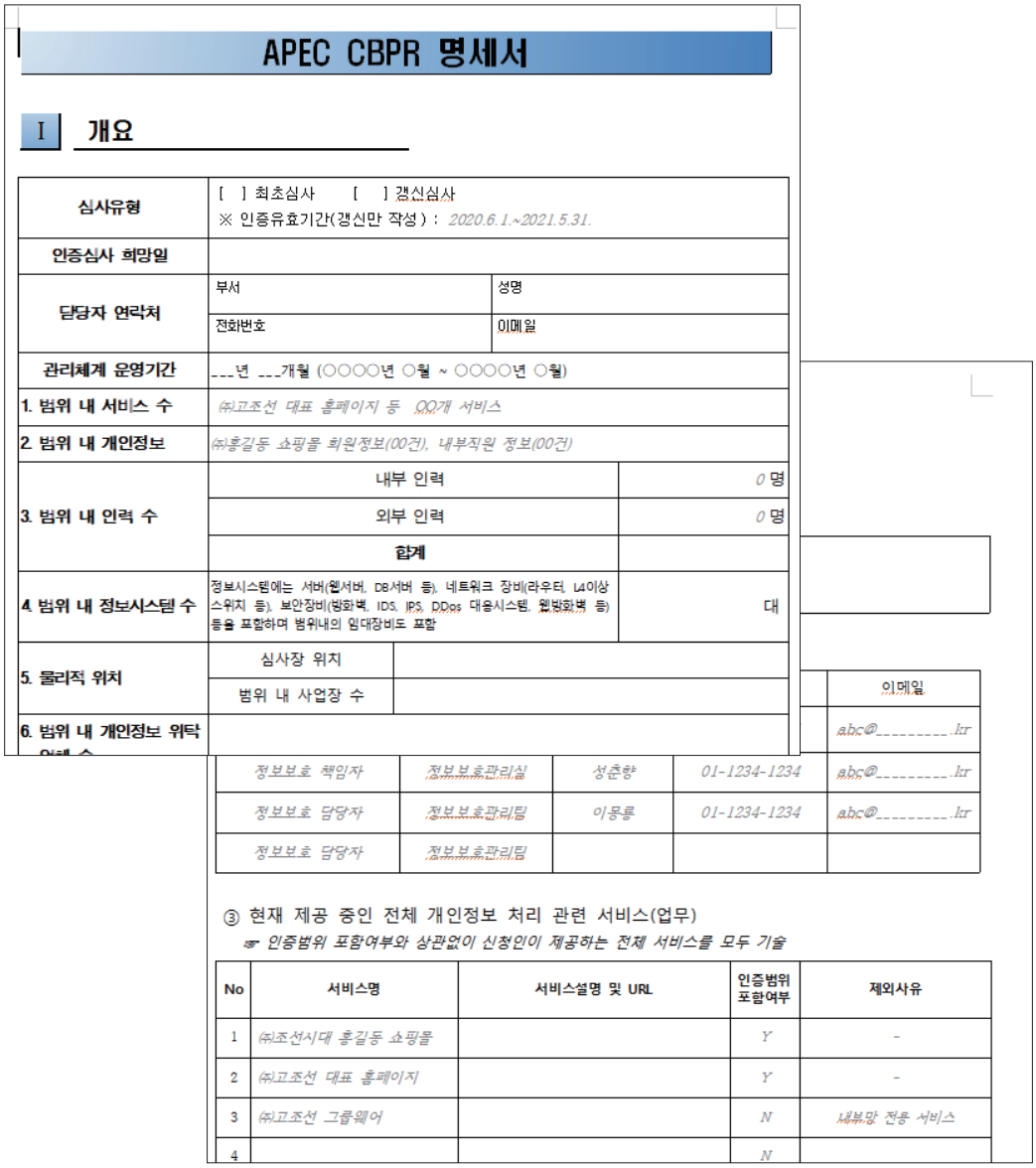
APEC CBPR 인증을 위와 같이 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원장 귀하

- **(CBPR 명세서)** CBPR 명세서는 신청인의 개인정보 처리와 관련된 현황을 작성한다. 인증 신청 범위 내의 개인정보 처리 업무, 설비, 인력 및 조직 등에 대한 현황, 개인정보 처리 규모/흐름도, 관리체계 관련 주요 조치 이력, 문서 목록 등에 대해 정보를 기재한다.



APEC CBPR 명세서

Ⅰ 개요

심사유형	[ ] 최초심사 [ ] 갱신심사 ※ 인증유효기간(갱신만 작성) : *2020.6.1.~2021.5.31.*	
인증심사 희망일		
담당자 연락처	부서	성명
	전화번호	이메일
관리체계 운영기간	___년 ___개월 (○○○○년 ○월 ~ ○○○○년 ○월)	
1. 범위 내 서비스 수	*㈜고조선 대표 홈페이지 등 00개 서비스*	
2. 범위 내 개인정보	*㈜홍길동 쇼핑몰 회원정보(00건), 내부직원 정보(00건)*	
3. 범위 내 인력 수	내부 인력	*0* 명
	외부 인력	*0* 명
	합계	
4. 범위 내 정보시스템 수	정보시스템에는 서버(웹서버, DB서버 등), 네트워크 장비(라우터, L4이상 스위치 등), 보안장비(방화벽, IDS, IPS, DDos 대응시스템, 웹방화벽 등) 등을 포함하며 범위내의 임대장비도 포함	대
5. 물리적 위치	심사장 위치	
	범위 내 사업장 수	
6. 범위 내 개인정보 위탁 업체 수		

				이메일
				abc@_____.kr
정보보호 책임자	*정보보호관리실*	*성춘향*	*01-1234-1234*	*abc@_____.kr*
정보보호 담당자	*정보보호관리팀*	*이몽룡*	*01-1234-1234*	*abc@_____.kr*
정보보호 담당자	*정보보호관리팀*			

③ 현재 제공 중인 전체 개인정보 처리 관련 서비스(업무)

☞ 인증범위 포함여부와 상관없이 신청인이 제공하는 전체 서비스를 모두 기술

No	서비스명	서비스설명 및 URL	인증범위 포함여부	제외사유
1	*㈜조선시대 홍길동 쇼핑몰*		*Y*	-
2	*㈜고조선 대표 홈페이지*		*Y*	-
3	*㈜고조선 그룹웨어*		*N*	*내부망 전용 서비스*
4			*N*	

- **(자가 평가지)** CBPR의 50가지 인증기준에 대한 신청인의 이행현황을 작성한다. 각 기준에 대한 보충 설명과 참고할만한 ISMS-P의 통제 항목을 맵핑하였으며, 이에 대한 신청인의 이행현황을 상세히 작성한다. 또한 이를 입증할 수 있는 내부 정책 문서, 이행 계획/결과물 등 증적자료 목록을 상세히 기재한다.

APEC CBPR 자가평가 질문지

CBPR 기준					신청인 이행 현황		
분야	항목	요구 사항	추가 설명 및 관련 준비자료	관련 ISMS-P 인증기준	이행여부 (Y/N/해당없음)	이행 현황	증적자료 (내부 정책 문서, 결과물 등)
※ 참고 : 세번째 컬럼의 1~50번까지 숫자는 CBPR 원본(영문) 자가평가 질문지 상의 번호(CBPR의 9가지 보호원칙 기준으로 분류되어 순번 정렬)							
1. 개인정보 관리 체계 수립(2)							
1.1 정책 수립	1.1.1 CBPR 이행 근거 규정	39. CBPR의 보호 원칙의 책임있는 준수를 위해 이의 근거가 되는 개인정보보호 관련 내부 지침 또는 법규 등의 준거 규정이 있어야 한다.	o CBPR 보호 원칙을 포괄하는 내부 지침 또는 법규, 규칙 등 준거 규정이 있어야 한다. - 개인정보보호 관련 내부 지침 또는 정책 - 개인정보 처리와 관련하여 외부기관 또는 내부 직원 등과 체결한 계약 - 관할 개인정보보호 관련 법규 - 관할 개인정보보호 관련 자율규제 프로그램/행동규약 <관련 준비자료> • 개인정보보호 관련 내부 정책/지침 • 개인정보처리 위수탁 계약서 및 직원 보안 서약서 등 • 개인정보보호 관련 적용 대상 법규 • 참여 중인 개인정보보호 관련 자율규제 프로그램/행동규약	1.1.5(정책 수립) 정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다. 1.4.1(법적 요구사항 준수 검토) 조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.			
1.2 책임자 지정	1.2.1 개인정보보호 책임자 지정	40. CBPR의 보호원칙 준수를 총괄하는 책임자를 지정해야 한다.	o CBPR 보호원칙 준수 등 개인정보보호 업무를 총괄하는 개인정보보호책임자를 지정하고 개인정보보호 업무를 체계적으로 이행하는 조직을 구성해야 한다. 책임자의 업무는 개인정보와 관련된 민원 대응 업무를 포함해야 한다. <관련 준비자료> • 개인정보 보호 책임자 지정 및 역할과 관련한 내부 정책/지침 • 개인정보보호 조직도 • 개인정보 보호책임자 임명 관련 자료(인사기록카드, 인사명령 등)	1.1.2(최고책임자의 지정) 최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.			

- 신청서류는 이메일, 방문접수 또는 등기우편으로 제출할 수 있으며, 신청 서류의 미비로 인증 또는 신청인의 보완요청이 있을 경우 신청 서류를 재구비하여 제출하여야 한다. 인증을 받고자 하는 인증심사 대상 서비스가 여러 개 있는 경우 인증 범위를 합치거나 분할하여 신청할 수 있다. 인증심사 신청부터 인증심사까지 예비 점검, 심사원 모집 등 업무처리를 위한 기간이 필요하므로 희망심사일 기준 최소 8주전에 신청해야 한다.

- **(확약서)** 인증 신청인이 인증심사 과정 또는 인증서 획득 이후의 책임과 의무에 대한 내용을 기술한 것으로 인증심사 중단, 인증 취소 사유에 해당하는 행위 등이 포함되어 있다. 신청인은 확약서 내용을 숙지하고 서명(대표자)하여 제출한다.

2.1.3 예비 점검 준비

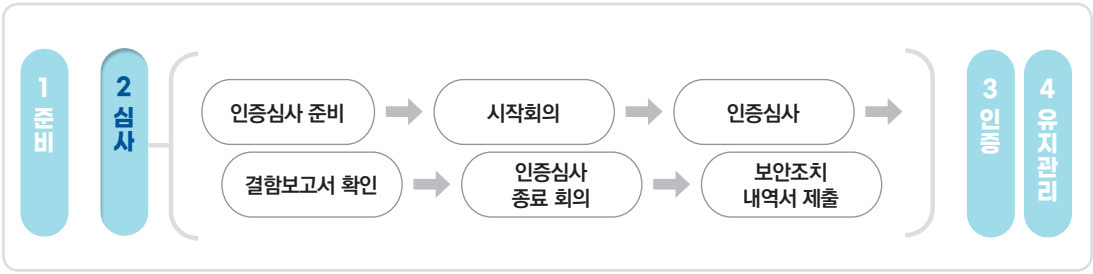
- 예비 점검이란 심사팀장이 신청인을 방문하여 개인정보처리시스템의 규모, 위험 식별 및 평가 수행 여부, 운영명세서 등 인증심사에 필요한 기초자료 구비 유무, 인증심사 준비상태 및 운영 여부를 확인하는 것이다. 신청인은 다음의 세부 점검 사항을 확인하고 준비한다.

점검 항목	세부 점검 사항
인증 범위 적정성	• 전체 업무 및 인증 범위 내 업무 확인 • 인증서 등에 반영될 인증 범위명 확인 • 인증 범위 내 누락 정보자산 및 네트워크 구성 확인 ※ CBPR 명세서, 자가평가지 기반으로 점검
조직(구성원) 현황	• 인증 범위 내 업무, 조직 및 인원의 누락 여부 확인 • 정보보호 및 개인정보 보호 전담조직 현황 확인
물리적 현황	• 인증 범위 내 사무실, 전산실 등의 물리적인 위치
CBPR 운영 현황	• [정책] 정책체계 및 정책/지침/매뉴얼 운영 여부 확인 • [위험분석] 인증심사 전 위험분석 및 평가, 개인정보 보호대책 수립 및 이행 여부 확인 • [자가 평가지] 자가 평가지 작성 및 N/A 항목 적정성 확인 • [이행 증적] CBPR 이행 증적 자료 확인(1개월 이상)
자가 진단 내용	• 홈페이지 등 온라인 점검 • 개인정보의 기술적 취약점 점검 • 개인정보의 오남용 방지를 위한 모니터링 등의 방법 등

- 심사팀장은 예비 점검을 통해 인증 범위의 적정성, 인증심사 전 필수 수행사항 및 운영 현황 등을 확인하고 심사 진행 여부를 결정한다. 최종적으로 신청인의 개인정보 보호책임자(CPO) 또는 정보보호 최고책임자(CISO) 및 담당자와 예비 점검 결과를 공유하고, 인증 범위를 고려하여 심사 일정을 확정한다.

- 심사진행이 결정된 이후 인증 범위, 심사 기간 등을 협의한다. KISA는 인증심사에 소요되는 비용을 신청인에게 청구할 수 있다.

2.2 인증심사



2.2.1 인증심사 사전준비

- 인증심사 전 인증 또는 심사기관은 원활한 인증심사를 위해 심사계획을 수립하여 신청인에게 안내한다.
- 신청인은 안내된 심사계획에 따라 심사 장소, 심사대응 담당자 지정 및 심사 대응 협조 등을 사전에 준비해야 한다.

  ※ 출력물의 양이 많거나 여러 부를 준비하기 어려운 경우, 산출물 부수는 심사팀장과 협의하여 정할 수 있음

2.2.2 인증심사 시작회의

- 시작회의는 인증심사팀과 신청인의 CPO, CISO, 주요 부서장 및 직무자, 인증 담당자, 유관부서 관련자 등이 참석한다.
- 심사팀장은 CBPR 인증제도 개요, 심사원 소개, 심사 계획 등을 설명하고, 신청인 담당자는 CBPR 구축 및 운영 현황 등에 대하여 간략하게 설명한다.

2.2.3 인증심사

- 인증심사는 CBRP의 인증기준에 맞는 체계를 구축하고 적절하게 운영하고 있는지 확인한다.
- 인증심사는 서면심사와 현장심사를 병행하여 실시한다. 서면심사는 CBPR 관련 정책, 지침, 매뉴얼(절차) 등 내부규정 존재 여부 및 해당 내부 규정이 인증기준을 충족하는지 심사한다. 또한, 신청인에서 제출한 증적자료 확인이나 담당자 면담을 통해 운영의 적정성을 확인한다.

- 현장심사는 서면심사 진행 현황에 맞춰 일정을 조율하여 진행하며, 서면심사의 결과와 기술적·물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 등의 방법으로 심사한다.

인증심사 시 유의사항

- 인증심사 시 인증 준비 미흡 또는 인증심사팀 요청사항(추가자료 요청, 현장실사 및 인터뷰 요청 등) 대응이 미흡한 경우, 심사의 신뢰성을 확보할 수 없기 때문에 인증심사 중단 및 심사팀 철수가 이루어질 수 있다.

2.2.4 결함보고서 확인

- 인증심사팀은 서면 및 현장심사를 통하여 도출된 문제점에 대해 신청인 담당자와의 회의를 통해 상호간 결과를 확인한다.
- 신청인은 인증심사팀이 작성한 결함보고서에 사실과 다른 내용이 있는지 검토한다.
- 만약 중결함 사항이 확인된 경우 인증심사팀은 중결함이 확인된 시점부터 인증심사를 중단 할 수 있다.

결함 및 중결함 사항

- **결함 사항**: 신청인의 CBPR 인증심사기준에 규정된 요구사항을 충족하지 못하는 사항이 발견되고 있으나 발견된 문제점이 CBPR 운영에 중대한 영향을 미치지 않는 사항
- **중결함 사항**: 신청인의 CBPR 인증심사기준에 규정된 요구사항을 충족하지 못 하는 사항이 발견되고 있으며 발견된 문제점이 CBPR 운영에 중대한 영향을 미치는 사항

2.2.5 인증심사 종료회의

- 종료회의에서 인증심사팀은 신청인 임직원 및 담당자에게 심사 결과를 설명하고 보완 조치요청서를 통해 결함에 대한 보완조치를 요청한다. 보완조치 요청은 사정에 따라 심사종료 후 사후에 진행될 수도 있다.
- 인증심사팀은 보완조치 요청 및 기간, 보완조치 제출방법, 인증위원회 개최 등 향후 진행 사항 및 일정에 대하여 안내하는 것으로 심사를 종료한다.

2.2.6 보완조치 내역서 제출

- 신청인은 보완조치 요청을 받은 날로부터 40일 이내 보완조치를 완료하고 보완조치 사항에 대한 보완조치 내역서 및 보완조치 완료확인서를 작성하여 인증 또는 심사기관에 제출해야 한다.
- 인증 또는 심사기관이 제출된 보완조치 결과가 미흡하다고 판단하거나, 신청인 스스로 보완조치 내용상 기한 연장이 필요하다 판단되는 경우 공문을 통해 최대 60일(재조치 기간 포함) 연장할 수 있다. 보완조치 기한 연장 시 보완조치요약서 및 완료된 결함사항에 대한 보완조치 내역서를 공문과 같이 제출해야 한다.
- 최대 100일의 보완조치 기한은 심사팀장이 보완조치 결과를 확인하기 위한 이행점검이 완료된 시점까지 포함된다. 심사팀장은 보완조치 내역서의 적절성을 판단하고 이행점검을 통해 실제 이행 여부를 확인한다.
- 보완조치 완료 여부가 최종 확인된 이후 심사팀장은 확인 결과를 보완조치 완료 확인서에 각각 서명날인하고 보완조치 완료가 확인되었음을 신청인에 안내한다.
- 연장 기한 포함 최대 100일 내에 보완조치가 완료되지 않은 경우, 인증이 취소된다. (최초심사의 경우, 심사 무효)

인증심사 시 유의사항

- 인증 또는 심사기관은 신청인이 고의로 인증심사의 실시를 지연 또는 방해하거나 신청인의 귀책사유로 인하여 인증심사를 계속 진행하기가 곤란하다고 인정되는 경우 인증심사를 중단할 수 있다.

2.3 인증서 발급

2.3.1 인증위원회 심의·의결

- 인증심사에 따른 보완조치가 완료된 기관에 대하여 인증기관은 “인증심사 결과보고서”를 작성하여 인증위원회 안건으로 상정한다.
- 인증위원회는 한국인터넷진흥원 APEC CBPR 인증업무지침에 따라 관련 전문가로 구성되며 각 상정된 안건에 대하여 다음의 사항을 심의·의결한다.

CBPR 인증위원회 심의·의결 사항

- 인증심사 결과가 인증기준에 적합한지 여부
- 인증 취소 사유를 발견한 경우에 그 결과의 적합성 여부
- 그 밖에 CBPR 인증과 관련하여 위원장이 필요하다고 인정하는 사항

- 인증위원회에서는 심의 결과에 따라 보완조치를 요구할 수 있다. 이 경우 심사팀장을 통해 신청인에게 해당사항과 더불어 보완조치 기한이 전달된다.
- 보완조치사항을 전달받은 신청인은 해당사항의 보완 완료 후 심사팀장에게 수정된 "보완조치 내역서"를 제출해야 한다.
- 보완조치 이행 여부를 확인한 심사팀장은 해당사항에 대한 결과보고서를 다음 회기 인증 위원회에 상정하여 최종 인증부여 여부를 의결 받게 된다.
- 인증기관의 장은 인증위원회의 심의·의결 결과를 신청인에 통보하고 CBPR 인증기준에 적합한 경우 인증서를 발급한다. 인증서는 국문으로 발행이 되며 요청 시 영문 인증서 발급도 가능하다. 인증 부적합 통보를 받은 신청인은 이에 대해 이의신청을 할 수 있다.

CBPR 인증 마크 및 인증서 양식



APEC CBRP 인증서

1. 인증번호 :
2. 업체명 :
3. 대표자 :
4. 인증의 범위 :
5. 유효기간 :

위와 같이 APEC CBPR 인증을 부여합니다.

년 월 일

한국인터넷진흥원장 직인

2.3.2 인증서 수령

- 인증 취득 기업은 CBPR 인증 유효기간 동안 개인정보 보호 관리체계를 지속적으로 유지하고 관리하여야 한다. 인증 취득 기업은 인증 범위와 관련하여 개인정보 침해 사고 발생 또는 인증기관에 접수된 민원 처리 등을 위해 인증기관이 요구하는 사항(사실 확인, 시정 요구 등)에 성실히 대응하여야 한다.

2.4 인증 유지·관리



2.4.1. 인증서 갱신 신청

- CBPR 체계 인증의 유효기간은 1년이며 인증을 유지하기 위해서는 인증 유효기간 만료 전에 갱신 신청을 해야 한다. 따라서 유효기간 2~3개월 이전에 갱신 심사 신청 준비를 하는 것이 바람직하다.
- 인증 유효기간 내 갱신 심사를 신청하였으나 인증서 유효기간 이후에 갱신이 완료되는 경우에도 인증은 유지되며, 이때 인증 유효 기간은 실제 인증서 갱신일이 아닌 이전 유효기간 이후부터 계산된다.
- 갱신 심사는 최초 심사와 동일한 기준과 절차로 진행되며 인증위원회에서 인증 유효기간 연장에 대한 심의·의결을 받도록 하고 있다.



APEC CBPR 인증

국경 간 개인정보 처리에 관한 인증 안내서

PART III

CBPR 인증기준

1. 개인정보 관리 체계 수립
2. 개인정보 수집
3. 개인정보 이용/위탁/제공
4. 정보주체 권리
5. 무결성
6. 보호 대책

III CBPR 인증기준

- CBPR은 개인정보 관리체계 수립에서부터 개인정보 수집, 개인정보 이용·위탁·제공, 정보주체의 권리, 무결성, 보호 대책 등 개인정보 처리 단계 또는 보호 대책 유형에 따라 6개 분야 총 50가지 인증기준으로 구성되었다.

※ APEC의 영문 CBPR 인증기준은 APEC 프라이버시 보호 원칙 별로 8개 분야로 분류되어 구성되었으나, 일반적인 개인정보 처리 관행 등을 고려하여 개인정보 처리 흐름별 개인정보 요구 사항을 쉽게 파악할 수 있도록 이와 같이 인증기준을 재구성하였다.

CBPR 인증기준

분야(6)	세부 항목(50)	
1. 개인정보 관리 체계 수립(2)	1.1 정책 수립	1.1.1 CBPR이행 근거 규정
	1.2 책임자 지정	1.2.1 개인정보 보호 책임자 지정
2. 개인정보 수집(9)	2.1 최소 수집	2.1.1 개인정보 수집 경로
		2.1.2 개인정보 최소 수집
		2.1.3 합법적 수집
	2.2 개인정보 처리방침	2.2.1 개인정보 처리방침 공개
	2.3 수집 시 고지	2.3.1 수집 고지_수집항목
		2.3.2 수집 고지_수집목적
		2.3.3 수집 고지_위탁/제공
		2.3.4 선택권 고지_눈에 띄게 표시
		2.3.5 선택권 고지_쉽게 설명

분야(6)	세부 항목(50)	
3. 개인정보 이용/제공/위탁(7)	3.1 이용	3.1.1 목적 내 이용
		3.1.2 목적 외 이용
	3.2 제공/위탁	3.2.1 제공 여부
		3.2.2 위탁 여부
		3.2.3 목적 내 제공/위탁
		3.2.4 목적 외 제공/위탁
	3.3 자료 제출 요구 대응	3.3.1 자료 제출 요구 대응
4. 정보주체 권리(11)	4.1 열람권	4.1.1 개인정보 보유 여부 확인권
		4.1.2 열람권
	4.2 정정/삭제권	4.2.1 정정/완성/삭제권
	4.3 선택권	4.3.1 수집 제한
		4.3.2 이용 제한
		4.3.3 제3자 제공 제한
		4.3.4 선택권 행사
		4.3.5 선택권 조치
	4.4 민원제기	4.4.1 민원 처리 절차
		4.4.2 민원 처리 기한
		4.4.3 민원 처리
5. 무결성(5)	5.1 최신성 유지	5.1.1 최신성 검증
		5.1.2 최신화
	5.2 최신정보 공유	5.2.1 수탁사에 통지
		5.2.2 제3자에 통지
		5.2.3 수탁사로부터 통지
6. 보호 대책(16)	6.1 보호대책 수립/이행	6.1.1 보호대책 수립
		6.1.2 보호대책 구현
		6.1.3 비례적 보호대책
		6.1.4 보호대책 이행
		6.1.5 보호대책 요구사항
	6.2 보호대책 평가/개선	6.2.1 보호대책 평가
		6.2.2 보호대책 개선
	6.3 수탁사의 보호대책	6.3.1 수탁사 보호체계
		6.3.2 수탁사 보호대책
		6.3.3 수탁사 보호조치 요구사항
		6.3.4 수탁사 관리·감독(자체평가)
		6.3.5 수탁사 관리·감독(현장점검)
	6.4 제3자의 보호대책	6.4.1 제3자의 보호조치
	6.5 파기	6.5.1 파기
	6.6 임직원 인식제고	6.6.1 임직원 인식제고
		6.6.2 임직원 교육

1. 개인정보 관리 체계 수립

1. 개인정보 관리 체계 수립

1.1 정책 수립 | 1.2 책임자 지정

1.1 정책 수립

1.1.1 CBPR 이행 근거 규정

39*. CBPR의 보호 원칙의 책임 있는 준수를 위해 이의 근거가 되는 개인정보 보호 관련 내부 지침 또는 법규 등의 준거 규정이 있어야 한다.

* 여기에 표기된 숫자는 CBPR 원본(영문) 자가평가 질문지 상의 번호(CBPR의 9가지 보호원칙 기준으로 분류되어 순번 정렬)

주요 확인사항

- CBPR의 개인정보 보호 원칙 이행을 위한 내부 또는 외부 근거 규정 또는 지침 등이 있는가? (예 : CBPR 원칙이 반영된 내부지침 마련, 법령의 준수, 자율규제 규약 또는 계약서의 이행 등)
- 위의 근거 규정 또는 지침에 대한 주기적인 점검 또는 외부 규정의 개정, 변경 등에도 CBPR의 개인정보 보호 원칙 이행이 보장되도록 확인하는가?

- CBPR의 개인정보 보호 원칙이 안정적이고 실질적으로 이행될 수 있도록 이행의 근거가 되는 내부 또는 관할 법령 등 외부 규정이 있어야 한다.
- 먼저 신청인의 모든 개인정보 보호 활동에 관한 근거를 포함하는 내부 개인정보 보호 정책 또는 규정을 마련하여야 한다. 내부 정책/규정은 조직의 개인정보 처리에 관한 최상의 문서로서, 개인정보 처리 원칙, 보호대책뿐만 아니라 개인정보 보호에 관한 조직 운영, 이행 및 점검 체계 등의 사항이 포함되어야 한다. 분야별 세부 이행 사항에 대해서는 하위 실행 문서를 통해 구체적인 가이드를 마련할 수 있다.

- 구속력이 있는 관할 법령, 분야별 규약 또는 신청인이 참여하는 자율규제 프로그램 등을 준거 규정으로 하는 경우, 해당 규정이 CBPR의 개인정보 보호 원칙에 위배됨이 없어야 한다. 만일 CBPR 원칙을 모두 충족하지 못하는 경우는 별도의 내부 규정/지침을 마련하여 이에 맞는 개인정보 관리에 대한 체계를 마련해야 한다. 또한 이러한 관할 법령이나 규약 등의 개정이나 관련 환경 변화 등에도 CBPR 원칙 이행이 보장될 수 있도록 주기적인 모니터링 등 필요한 추가 조치를 하여야 한다.

- 내부 개인정보 보호 정책은 최고 경영진의 승인을 받아 시행해야 하며, 모든 임직원이 쉽게 접근할 수 있도록 사내 게시판에 게시하거나 책자로 배포하는 등의 조치를 취하여야 한다. 또한 내부관리계획은 연1회 이상 주기적으로 그 내용을 검토하여 최신화 하고 변경 이력을 기록하여야 한다.

증적 자료

- 개인정보 보호 관련 법적 준거성 검토 내역
- 개인정보 보호 정책/지침 및 검토, 개정 이력

결함 사례

개인정보 보호와 관련된 구속력 있거나 문서화된 근거없이 내부 개인정보 업무를 처리하는 경우

개인정보 보호법과 비교

- 개인정보 보호법은 개인정보 처리 시 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 내부 관리계획을 수립하고 이행하도록 하였다. 내부 관리계획에는 개인정보 보호책임자의 지정, 개인정보 취급자에 대한 교육, 개인정보 조직 구성·운영에 관한 사항을 비롯하여 개인정보의 기술적·관리적·물리적 보호를 위한 조치 사항이 포함되어야 한다.

법령

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제29조(안전조치 의무)
- 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
- 개인정보의 안전성 확보조치 기준 및 해설서('20.12월)

관련 ISMS-P 인증기준

- 1.1.5(정책 수립) 정보보호와 개인정보 보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보 보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
- 1.4.1 (법적 요구사항 준수 검토) 조직이 준수하여야 할 정보보호 및 개인정보 보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.

1.2 책임자 지정

1.2.1 개인정보 보호책임자 지정

40. CBPR의 보호원칙 준수를 총괄하는 책임자를 지정해야 한다.

주요 확인사항

■ 개인정보 보호 처리에 관한 업무를 총괄하는 개인정보 보호책임자를 공식적으로 지정하고 있는가?

■ 신청인은 개인정보 민원 처리 업무를 포함한 개인정보 보호책임자의 업무 범위를 정하여 문서화하였는가?

- 신청인은 조직의 개인정보 업무 전체를 총괄하여 책임질 개인정보 보호책임자를 공식적으로 지정해야 한다. CBPR은 책임자가 될 수 있는 특정 지위 또는 자격 요건을 정하고 있지는 않으나, 관련 업무 수행 경력 등을 고려하여 개인정보 보호에 대한 전문성이 인정되는 자로 지정하되 개인정보 보호에 관한 예산, 정책을 결정하고 조직을 지휘할 수 있는 권한이 주어져야 한다. 국내 개인정보 보호법을 참고하여 개인정보 처리 관련 업무를 수행하는 부서의 장이나 관련 임원을 책임자로 지정하여 개인정보 보호 관련 인력, 예산 등을 할당할 수 있는 권한이 있는 자로 지정하는 것도 고려할 수 있다.
- 개인정보 보호책임자는 개인정보 민원 처리를 비롯하여 개인정보 보호 정책의 수립, 개인정보 보호 정책 이행에 대한 관리·감독 및 임직원 대상 개인정보 보호 교육 시행 등 구체적인 책임자의 역할과 권한을 정하고 내부 개인정보 보호정책 등에 명시하여야 한다. 이때 다음의 개인정보 보호법의 개인정보 보호책임자의 역할을 참고하여 마련할 수 있다.

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 개인정보 보호책임자의 자격 요건, 역할 등에 대해 구체적으로 명시하고 있다. 먼저 기관의 대표 또는 임원을 개인정보 보호책임자로 지정할 수 있으며, 임원이 없는 경우 개인정보 처리 관련 업무를 담당하는 부서의 장이 이를 대신하도록 했다. 책임자의 역할은 다음과 같이 규정했다.
  - 개인정보 보호 계획의 수립 및 시행
  - 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
  - 개인정보 처리와 관련한 불만의 처리 및 피해 구제
  - 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
  - 개인정보 보호 교육 계획의 수립 및 시행
  - 개인정보파일의 보호 및 관리·감독
  - 개인정보 처리방침의 수립·변경 및 시행
  - 개인정보 보호 관련 자료의 관리
  - 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

증적 자료

- 개인정보 보호 책임자 지정 및 역할과 관련한 내부 정책/지침
- 개인정보 보호 조직도
- 개인정보 보호책임자 임명관련 자료(인사기록카드, 인사명령 등)

결함 사례

- 개인정보 보호책임자를 지정하였으나 내부 정책 등에 책임자의 역할이 구체적으로 명시되지 않은 경우

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제31조(개인정보 보호책임자의 지정)
- 개인정보 보호법 시행령 제32조(개인정보 보호책임자의 업무 및 지정요건 등)

• 관련 ISMS-P 인증기준 •

- 1.1.2 (최고책임자의 지정) 최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보 보호 업무를 총괄하는 개인정보 보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.

2. 개인정보 수집

2. 개인정보 수집

- 2.1 개인정보 수집
- 2.2 개인정보 처리방침 공개
- 2.3 개인정보 수집

2.1 최소 수집

2.1.1 개인정보 수집 경로

5. 개인정보를 수집하는 경로를 쓰시오.

5.a) 정보주체로부터 직접 수집
5.b) 수탁사로부터 수집
5.c) 기타 다른 방법

주요 확인사항

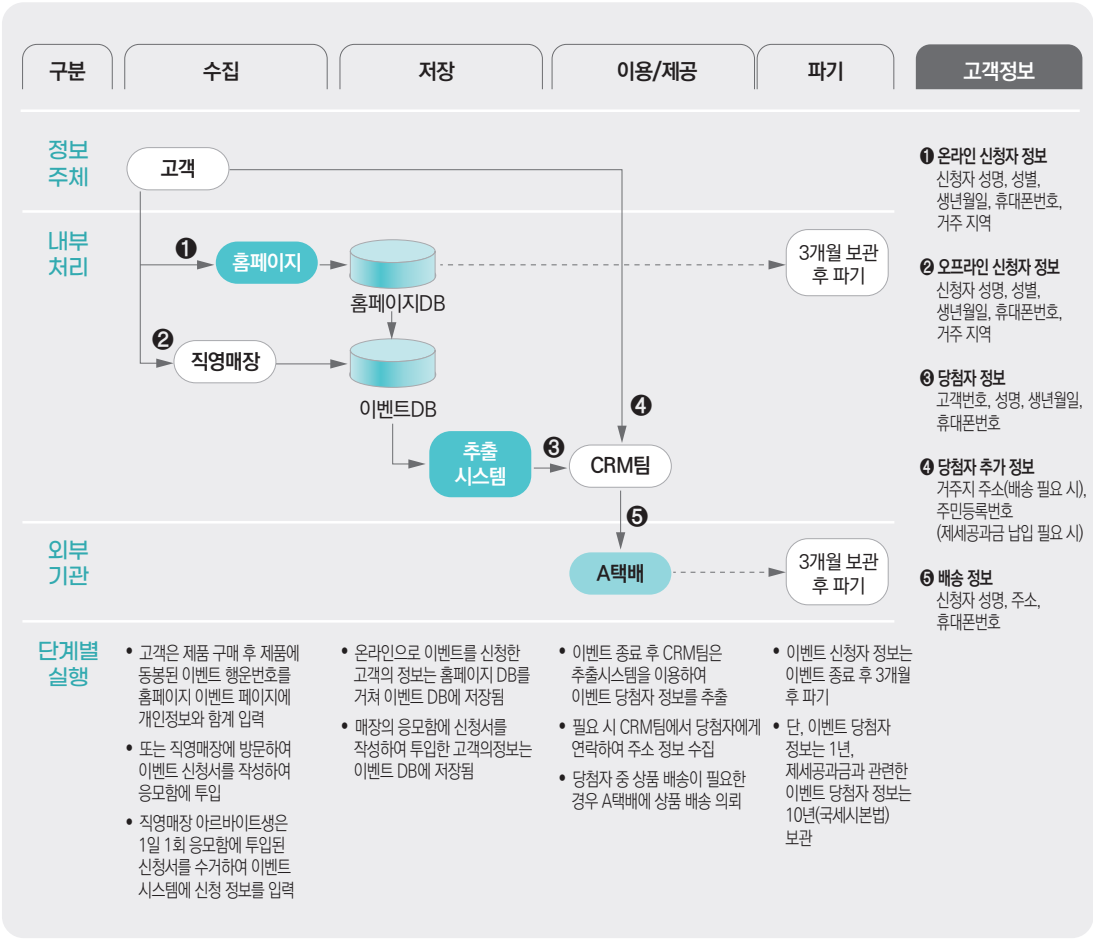
■ 신청인은 어떤 경로를 통해 개인정보를 수집하고 있는가?
■ 신청인은 (인증 범위 내) 모든 개인정보 수집 경로를 개인정보 흐름도에 명시하였는가?

해설

- 신청인은 인증 범위 내 모든 개인정보의 수집 과정을 포함하는 개인정보 흐름도를 작성하여 제시하여야 한다.
  - 온라인 수집 : 홈페이지 등을 통한 회원가입, 제품 구매, 문의사항 작성 등
  - 오프라인 수집 : 가입신청서, 계약서, 응모권 등 서면 양식 등
  - 수탁사 등을 통한 수집 : 상담(전화, 이메일, 온라인·앱 등), 이벤트 대행 등
  - 제3자로부터의 제공(공유)받는 경우 등

- 아래 예시는 이벤트 신청 및 당첨자 추출에 관한 개인정보 흐름도이다
  - 개인정보의 흐름도에는 개인정보의 처리단계(수집, 저장, 이용, 제공, 파기)에 따라 처리되는 개인정보 항목, 처리와 관련된 주체 및 관련시스템, 위·수탁사가 명시되어 있다.

개인정보 흐름도 예시: 이벤트 신청 및 담청자 추출



증적 자료

- 개인정보 수집에 관련한 내부 개인정보 정책/지침
- 개인정보 흐름도

결함 사례

- 제휴사(제3자)를 통해 수집하는 개인정보의 처리 과정이 개인정보 흐름도에 누락된 경우

• 개인정보 보호법과 비교 •

- 해당 사항 없음

• 법령 •

관련 개인정보 보호법 법조항 및 지침 등

- 해당 사항 없음

• 관련 ISMS-P 인증기준 •

- 1.2.2 (현황 및 흐름분석) 관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.

2.1.2 개인정보 최소 수집

6. 개인정보 수집 시 수집 목적 달성 또는 목적과 관련된(compatible or related) 범위에 적합한 개인정보만 수집해야 한다.

주요 확인사항

- ■ 신청인은 개인정보 수집 목적 달성 또는 목적과 관련된 범위에 필요한 정보만을 수집하고 있는가?
- ■ 각 수집하는 개인정보 항목 별 수집 목적과 처리 내용이 명시되어 있는가?
- ■ 개인정보 수집 목적 이외 이와 관련된 목적으로 개인정보를 처리하는 경우 이의 관련성에 대한 근거를 제시하는가?

- 신청인은 개인정보를 수집할 때는 신청인이 명시한 처리목적에 필요한 개인정보에 한해 수집하여야 한다. 이때 각 개인정보의 수집·이용 목적이 식별되도록 수집 목적별 수집하는 개인정보 항목을 명시한다. 이때 해당 개인정보가 처리 목적에 필요한 것인지 여부는 처리 목적 달성 가능성과 비례하여 평가될 수 있으며 이를 입증할 책임은 개인정보처리자에게 있다.
  - 예를 들어, 직원 채용 시, 채용을 위한 지원자의 경력, 전공분야, 자격증 보유 정보 등에 관한 정보는 업무능력 판단을 위한 필수적이고 최소한의 정보로 볼 수 있으나, 지원자의 가족관계, 결혼 유무 등에 관한 정보를 수집한 경우 최소 정보의 범위를 벗어난다.

- 수집하는 목적에 필요한 개인정보 항목의 수집은 간접수집(제3자로부터 제공받거나 서비스 이용 중에 수집·생성되는 경우)시에도 동일하게 적용된다.

- 정보주체의 명시적 동의를 받은 경우 필요 최소한의 정보 이외의 정보도 수집하거나 이용할 수 있지만, 필요 최소한의 정보 이외의 정보를 필수 수집항목에 포함하여 수집할 수 없으며, 선택항목으로 별도로 분리하여 동의 받아 수집하여야 한다. 이 때 정보주체가 선택항목에 대하여 수집 거부의사를 밝혀도 신청인이 제공하는 해당 본질적인 서비스 이용에 지장이 없어야 한다.

증적 자료

- 개인정보 수집 목적별 처리하는 개인정보 항목(또는 수집 항목별 처리 목적)에 관련한 내부 정책/지침

결함 사례

- 온라인 쇼핑몰 회원 가입 단계에서 주소 정보를 필수적으로 수집하고 있는 경우(주소 정보는 물품을 구매하는 단계에서 필수적으로 수집하면 되며, 가입 단계에서는 필수항목으로 수집할 이유가 없음)
- 개인정보 수집 목적이 포괄적으로 기술되어 수집되는 개인정보 항목이 처리 목적 달성에 필수적인지 여부가 식별이 어려운 경우

개인정보 보호법과 비교

- 개인정보 보호법 또한 개인정보를 수집할 때에는 그 목적에 필요한 최소한의 개인정보를 수집하도록 규정하고, 필요 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다고 해서 정보주체에게 재화 또는 서비스의 제공을 거부해서는 안 된다고 명시했다. 최소한의 개인정보 수집이라는 입증 책임 또한 개인정보처리자가 부담한다.

2.1.3 합법적 수집

7. 개인정보 수집에 관한 관할 법령과 일관성을 이루고, 합법적이고 공정한 방법으로 개인정보를 수집해야 한다.

주요 확인사항

- ■ CBPR의 개인정보 보호 원칙에 따라 합법적이고 공정한 절차로 개인정보를 수집하는가?
- ■ 개인정보 처리 관련 관할 법령을 인지하고 이를 준수하고 있는가?

- 개인정보를 수집할 때에는 CBPR의 개인정보 보호 원칙을 준수하는 공정하고 합법적인 절차로 수집해야 한다. 따라서 개인정보 처리 목적과는 관계없는 개인정보 제공을 조건부로 서비스 가입을 유도하거나 정보주체가 개인정보 수집 사실이나 목적을 인지하기 어려운 방법이나 또는 기타 부정한 수단으로 개인정보를 수집하여서는 안 된다.

- 또한 신청인은 해당 개인정보 처리에 적용되는 관할 개인정보 보호 법령을 식별하고 이를 내부 개인정보 보호 정책 등에 반영하여 준수하여야 한다.

증적 자료

- 개인정보 수집 절차 및 근거에 대한 내부 정책/지침
- 관련 개인정보 보호 법령 식별 및 이의 이행에 대한 내부 정책/지침
- 개인정보를 수집하는 각종 양식(온라인 회원가입 화면, 서면 계약서/신청서, 전화 고객 상담 접수 매뉴얼 등)

결함 사례

- 서비스나 상품의 제공에 있어 해당 개인정보의 처리와는 직접적인 관련이 없음에도 개인정보 제공을 조건으로 이러한 서비스나 상품을 제공하는 경우
- 개인정보 수집 절차와 근거가 관할 개인정보 보호 규정의 요구 사항에 위배되는 경우

개인정보 보호법과 비교

- 개인정보 보호법은 세부 개인정보 보호 규정의 토대가 되는 개인정보 보호의 기본 원칙을 수립하였으며, 개인정보 처리 목적의 명확화, 목적 내 이용 원칙 등을 비롯하여 개인정보처리자가 최소한의 개인정보를 적법하고 정당하게 수집하도록 하는 원칙 등이 있다.

관련 법령

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제3조(개인정보 보호 원칙)

관련 ISMS-P 인증기준

- 3.1.1(개인정보 수집 제한) 개인정보는 서비스 제공을 위하여 필요한 최소한의 정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다.

2.2 개인정보 처리방침 공개

2.2.1 개인정보 처리방침 공개

1. 개인정보 처리 방법과 정책에 대한 개인정보 처리방침 등을 수립하고 정보주체가 명확히 이해하고 확인하기 쉬운 방법으로 공개해야 한다.

- 개인정보 처리방침에는 다음의 사항이 포함되어야 한다.
  - 수집하는 개인정보 항목 및 수집 방법
  - 개인정보 수집·이용 목적
  - (해당하는 경우) 제3자 제공 또는 업무 위탁 사실 및 세부 내용(제공/위탁 목적, 제공/위탁 기관 등)
  - 기관명, 위치 및 개인정보 보호 담당자 또는 책임자의 연락처
  - 정보주체의 개인정보 열람·정정 권리 등 권리행사 방법

주요 확인사항

- ■ 신청인의 개인정보 처리에 관한 관행 및 정책의 주요 사항을, 일반에게 공개할 목적으로 문서화한 개인정보 처리방침을 마련하였는가?
- ■ 개인정보 처리방침을 정보주체가 명확히 이해하고, 확인하기 쉬운 방법으로 공개하는가?
- ■ 개인정보 처리방침에는 개인정보 수집이용 및 위탁·제공에 관한 사항, 정보주체의 권리 및 신청인의 연락처 등이 포함되었는가?
- ■ 개인정보 처리방침의 시행일을 표시하고, 개인정보 처리 관행 및 정책 등의 변경에 따라 최신의 상태로 유지하는가?

- (개인정보 처리방침 마련) 신청인은 정보주체를 포함한 일반인이 신청인의 개인정보 처리에 관한 관행이나 보호 정책의 주요 내용을 쉽게 알 수 있도록 개인정보 처리방침을 마련하여 공개해야 한다.

- (공개) 개인정보 처리방침을 공개할 때에는 정보주체가 쉽게 확인할 수 있도록 신청인의 홈페이지 첫 페이지에 링크 등을 통해 눈에 띄기 쉬운 곳에 게시한다. 인터넷 홈페이지에 게시하기 어려운 경우는 관련 계약서 등 개인정보를 수집하는 경로나 매체에서 정보주체가 접근하기 쉬운 곳에 공개한다. 또한 일반적인 서비스 범위가 아닌 특정 분야에만 적용되는 개인정보 처리방침을 별도 운영하는 경우에는 해당 개인정보 처리 관련 페이지 등에 게시할 수 있다. 처리방침에 공개되는 내용은 정보주체가 이해하기 쉽도록 쉬운 언어로 표현하여야 한다.

- (고지 사항) 개인정보 처리방침에는 개인정보 수집·이용 및 제공·위탁 등의 처리에 관한 사항, 정보주체의 개인정보 열람·정정 및 삭제권리에 관한 사항을 비롯하여 개인정보 보호 담당자 연락처 등 다음의 사항이 포함되어야 한다.

개인정보 처리방침 내 고지 사항

- 수집하는 개인정보 항목 및 항목별 수집 방법
- 개인정보 수집 항목별 수집·이용 목적
- (해당하는 경우) 개인정보 처리 업무 위탁 대상, 위탁 업무(목적)
- (해당하는 경우) 개인정보를 제공받는 기관(또는 유형), 제공 목적 등
- 기관명, 위치 및 개인정보 보호 담당자 또는 책임자의 연락처
- 정보주체의 개인정보 열람·정정 권리 등 권리행사 방법

  – 개인정보 수집·이용 목적 또는 개인정보 위탁·제3자 제공에 대한 고지 시에는 해당 처리되는 개인정보 항목별 목적 또는 처리 대상/목적별 개인정보 항목 등을 명시하여 정보주체가 명확하게 인지할 수 있도록 한다.

  – 이 외에도 개인정보 처리 및 보유기간, 개인정보 파기 방법, 쿠키 정보 수집에 관한 사항 및 안전성 확보 조치에 관한 사항 등을 공개하여 개인정보처리 관행 및 정책을 투명하게 운영할 수 있다.

- (최신성 유지) 개인정보 처리 관행이나 정책이 변경되는 경우 개인정보 처리방침의 해당 항목에 신속하게 반영하여 최신상태를 유지해야 한다. 또한 개인정보 처리방침 수립 또는 변경으로 방침의 효력이 발생하는 시행 일자를 명시한다.

증적 자료

- 개인정보 처리방침의 작성·공개에 대한 내부 정책/지침
- 개인정보 처리방침 링크 및 내용이 공개된 페이지 화면

결함 사례

- 직원 채용과 관련된 개인정보 처리 내용이 대표 홈페이지 또는 채용 홈페이지에 공개되어 있지 않는 경우
- 개인정보 처리방침을 확인할 수 있는 링크 또는 안내가 모바일 서비스에는 제공되지 않은 경우
- 고객센터 상담업무 중 전화를 통해서도 개인정보를 수집하고 있으나 해당 수집 방법이 개인정보처리 방침에 명시되어 있지 않은 경우
- 개인정보를 처리하는 수탁사의 수가 많거나 변경이 잦다는 이유로 수탁사의 이름, 수탁 업무 등 업무 위탁 현황을 모두 공개하지 않고 일부만 공개하는 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 개인정보 처리방침 공개를 의무화하고, 작성 및 공개 방법에 대해 구체적으로 명시하였다. 개인정보 처리방침을 공개할 때에는 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지에 동 명칭을 사용하고 글자크기, 색상 등을 활용하여 다른 고지사항과 구분되도록 하는 등 구체적인 방법을 정하였다. 또한 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우에도 사업장이나 정기 간행물을 통해 공개할 수 있도록 하였다.

- 개인정보 처리방침에 포함되어야 할 필수 고지 사항은 다음과 같다.

개인정보 처리방침 내 필수 기재사항

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항(시행령 제31조)
   1. 처리하는 개인정보의 항목
   2. 개인정보의 파기에 관한 사항
   3. 제30조에 따른 개인정보의 안전성 확보 조치에 관한 사항

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
- 개인정보 보호법 시행령 제31조(개인정보 처리방침의 내용 및 공개방법 등)
- 표준 개인정보 보호 지침(보호위 고시, '20.12)
- 개인정보 처리방침 작성 가이드라인(보호위, '20.12)

• 관련 ISMS-P 인증기준 •

- 3.5.1 (개인정보 처리방침 공개) 개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 개인정보 처리방침을 수립하고, 이를 정보주체(이용자)가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.

2.3 수집 시 고지

2.3.1 수집 고지_수집 항목

> 2. 개인정보를 수집하는 시점에 정보주체에게 수집하는 개인정보 항목을 고지해야 한다.

2.3.2 수집 고지_수집 목적

> 3. 개인정보를 수집하는 시점에 정보주체에게 개인정보의 수집 목적을 고지해야 한다.

2.3.3 수집 고지_위탁/제공

> 4. 개인정보를 수집하는 시점에 정보주체에게 개인정보를 제3자에게 위탁하여 처리 또는 제공될 수 있음을 고지해야 한다.

주요 확인사항

- ■ 신청인은 개인정보 수집 시점에 정보주체에게 개인정보의 수집 항목, 수집 목적 등을 고지하는가?
- ■ 신청인은 및 개인정보의 위탁 처리 또는 제3자 제공(또는 제공 가능성) 대해 알리는가?
- ■ 정보주체가 인지하기 쉽도록 합리적인 방법으로 고지하는가?

- 개인정보 수집·이용·제공에 대한 정보주체의 동의를 필수적으로 요구하지 않은 대신 합법적인 방법으로 수집하되 정보주체가 이를 명확하게 인지할 수 있도록 고지해야 한다. 그리고 추후 이러한 개인정보의 처리에 대해 정보주체가 선호에 따라 제한할 수 있도록 한다. 즉 개인정보 처리에 대한 사전 동의(opt-in) 원칙인 국내 개인정보 보호법과 구분되는 '옵트 아웃(opt-out)' 원칙의 보호 체계로 설명된다.

- **(고지 시점)** 신청인은 개인정보 '수집 시점'에 이러한 수집 또는 제3자 제공 사실을 정보주체에게 고지하여야 한다. 이는 신청인을 대신하여 개인정보 처리 업무를 하는 수탁자를 통해서 수집하는

경우에도 동일하게 적용된다.

- 개인정보를 수집하는 홈페이지의 화면, 가입신청서 등에 이와 같은 고지내용을 표시하여 정보주체가 사전에 이를 인지할 수 있도록 해야 한다.

- **(고지 내용)** 개인정보 수집·이용에 대한 고지 시에는 개인정보 수집 목적별 수집하는 개인정보 항목을 고지해야 하며, 개인정보를 제3자에게 제공하거나 제공할 가능성이 있는 경우에는 제공받는 대상별 제공목적, 제공항목 등을 구분하여 처리의 상세 내용에 대해 정보주체가 인지하기 쉽게 고지해야 한다.

적용 예외

- 다음의 경우에는 개인정보 수집 시 사전 고지 의무가 적용되지 않을 수 있으나 이러한 경우에도 가급적 고지하여 정보주체의 개인정보 침해 가능성을 최소화한다.
  - (암묵적 동의로 간주되는 경우) 정보주체가 개인정보 수집·이용·제공 사실, 목적 등을 명확하게 인지/예측이 가능하여 이러한 개인정보 처리에 대해 암묵적으로 동의하였다고 간주될 수 있는 상황의 경우(ex: 업무적 목적으로 명함 제공)
  - (공개적으로 이용 가능한 정보의 수집) 공개 명부 등 공개적으로 이용 가능한 정보를 그 공개된 목적으로 수집·이용하는 경우
  - (기술적 불가능) 잠재적 이용자의 초기 접속 등 전자 기술적으로 자동 수집되는 정보(쿠키 등)의 경우. 이 경우에도 가능한 빠른 시일 내 사후 고지해야 함
  - (법집행 기관에 제공되는 정보) 법집행 기관이 수사 목적으로 요청한 정보를 제공하는 경우로써, 이에 대한 고지가 수사에 방해될 것으로 예상되는 경우
  - (법적 절차에 따라 제공되는 정보) 소송 절차에 의한 요청 등 법적 절차, 양식에 의해 제공되는 개인정보의 경우
  - (제3자로부터 받은 정보) 제3자로부터 개인정보를 제공받은 경우
  - (합법적 조사 목적) 법령, 규약 등의 위반에 대한 내/외부 조사와 관련된 목적으로 개인정보 처리가 합리적으로 필요하고, 이에 대해 고지할 경우 정보 정확성이나 활용성이 침해될 것으로 예상되는 경우
  - (긴급 상황) 개인의 생명, 건강 또는 안전을 위협하는 긴급 상황에서 처리하는 개인정보의 경우

증적 자료

- 개인정보 수집 시 고지 또는 동의와 관련한 내부 정책/지침
- 개인정보를 수집하는 각종 양식(온라인 회원가입 화면, 서면 계약서/신청서, 전화 상담 접수 매뉴얼 등)

결함 사례

- 개인정보 수집 시 수집목적을 고지하고 있으나, 수집항목과 수집목적을 각각 구분하지 않아 각 개인정보 항목이 어떤 목적으로 수집·이용되는 지 확인이 어려운 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 개인정보처리자가 개인정보 수집·이용 또는 제3자 제공 시 정보주체로부터 개인정보 처리에 관한 다음의 사항을 고지하고 동의 받도록 했다.

개인정보 수집·이용 시 동의 항목	개인정보 제3자 제공 시 동의 항목
● 개인정보처리자(법 제15조) 1. 개인정보의 수집·이용 목적 2. 수집하려는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 ● 정보통신서비스 제공자(법 제39조의3) 1. 개인정보의 수집·이용 목적 2. 수집하는 개인정보의 항목 3. 개인정보의 보유·이용 기간	1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

- 이때 고지 내용은 개인정보 수집·이용 목적별, 제3자 제공에 대해서는 개인정보를 제공받는 자 별로 구분하여 상세 내용을 표기하도록 했다. 또한 정보주체에게 동의를 받을 때에는 수집하는 개인정보 항목, 홍보 목적의 연락, 민감 정보·고유 식별 번호의 사용 등 주요 내용에 대해서는 명확하게 표시하여 정보주체가 알아보기 쉽게 하도록 했다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제15조(개인정보의 수집·이용), 제22조(동의를 받는 방법)
- 개인정보 보호법 제39조의3(개인정보의 수집·이용 동의 등에 대한 특례)
- 개인정보 보호법 시행령 제17조(동의를 받는 방법)
- 개인정보 보호법 시행규칙 제4조(서면 동의 시 중요한 내용의 표시 방법)
- 개인정보 처리 방법에 관한 고시 제4조(서면 동의 시 중요한 내용의 표시 방법)

• 관련 ISMS-P 인증기준 •

- 3.1.2 (개인정보의 수집 동의) 개인정보는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다.

- 3.3.1 (개인정보 제3자 제공) 개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체(이용자)의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.

2.3.4 선택권 고지_눈에 띄게 표시

17. 정보주체가 개인정보의 수집, 이용 및 제공에 대한 선택권을 명확하게 인지할 수 있도록 눈에 잘 띄게 표시하여야 한다.

2.3.5 선택권 고지_쉽게 설명

18. 정보주체가 개인정보의 수집, 이용 및 제공을 제한할 수 있는 선택권에 대해 쉽게 이해할 수 있도록 알기 쉬운 문구로 고지해야 한다.

주요 확인사항

■ 정보주체가 선택권을 쉽게 인지하고 행사할 수 있도록 명확하고 눈에 잘 띄도록 고지하는가?

■ 선택권에 대한 고지는 쉽게 이해할 수 있는 문구와 방법으로 설명되었나?

- 신청인은 개인정보를 수집할 때는 정보주체가 해당 수집 사실, 목적 등에 대해 명확히 인지할 수 있도록 알려야 한다. 이에 더해 정보주체가 이러한 개인정보 처리를 제한하는 선택권이 있다는 사실과 이의 행사 방법에 대해서도 알려야 한다.
- 정보주체의 선택권을 고지할 때에는 제한할 수 있는 항목, 선택권 행사 방법 등에 대해 명확하고 눈에 띄는 방법으로 표시하고, 이해하기 쉽고 분명한 문구로 설명하여야 한다.

증적 자료

- 개인정보 수집·이용 및 제공과 관련한 온라인 가입화면, 서면 신청서 등
- 개인정보 선택권 관련 고지 내용

결함 사례

- 개인정보 처리를 제한하는 방법에 대해 모호하고 포괄적이거나 또는 어려운 용어로 설명하여 이해하기 어려운 경우
- 웹사이트 내 회원 가입 화면에 선택권에 대한 고지 링크가 표시되어 있으나 눈에 띄지 않는 크기와 위치에 표시된 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 개인정보 수집·이용 및 제공에 대한 정보주체의 동의 획득 원칙을 규정하고 있다. 동의를 받을 때에는 정보주체가 동의 내용에 대해 명확하게 이해할 수 있도록 내용과 형식을 규정하고, 특히 홍보 목적의 개인정보 처리, 민감정보 처리 등을 포함하여 다음의 주요 사항에 대해서는 다른 내용과 비교하여 명확히 알아보도록 표시하도록 했다.
  - 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
  - 처리하려는 개인정보의 항목 중 민감정보, 여권번호, 운전면허번호, 외국인등록번호
  - 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
  - 개인정보를 제공하는 경우 제공받는 자 및 제공받는 자의 개인정보 이용 목적

개인정보 처리에 대한 동의 획득 방법(개인정보 보호법 시행령 제17조)

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제15조(개인정보의 수집·이용)
- 개인정보 보호법 제17조(개인정보의 제공)
- 개인정보 보호법 제22조(동의를 받는 방법)
- 개인정보 보호법 시행령 제17조(동의를 받는 방법)

관련 ISMS-P 인증기준

- 3.1.2 (개인정보의 수집 동의) 개인정보는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다.

- 3.3.1 (개인정보 제3자 제공) 개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체(이용자)의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.

- 3.5.2. (정보주체 권리보장) 정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.

3. 개인정보 이용/위탁/제공

3. 개인정보 이용/제공/위탁

3.1 이용	3.2 제공/위탁
3.3 자료 제출 요구 대응	-

3.1 이용

3.1.1 목적 내 이용

8. 개인정보 처리방침 등에 고지한 개인정보의 수집 목적 또는 목적과 관련된 범위에 한하여 개인정보를 이용해야 한다.

3.1.2 목적 외 이용

9. 개인정보를 수집한 목적(또는 목적과 관련된 범위) 외 다른 목적으로 이용하는 경우, 정보주체의 명시적 동의나 다른 법률 근거 등 이에 대한 근거가 있어야 한다.

주요 확인사항

- ■ 개인정보 수집·이용 목적을 명확하게 고지하고 있는가?
- ■ 개인정보 수집 당시 정보주체에게 고지했거나 동의 받았던 이용 목적 또는 이와 관련된 목적에 한해서만 처리하고 있는가?
- ■ 개인정보 수집·이용 목적과 '관련된 목적'임을 판단하는 기준이나 근거가 있는가?
- ■ 만약 수집 당시 고지했던 이용 목적(또는 이와 관련된 목적) 외 개인정보를 이용하려는 경우 해당 이용에 대한 근거는 무엇인가? (예: 법령 근거 또는 정보주체의 동의 등 항목별 근거 제시)

- 개인정보 처리는 개인정보 수집 시 고지한 개인정보 수집·이용 목적 또는 이 목적과 양립가능하거나 관련된 목적 달성을 위한 경우에 가능하다. 이때 목적의 '양립가능성' 또는 '관련성'을 판단하는 기준은 원래의 목적에서 파생되거나 부가적인(further) 목적으로 이용되었는지 여부를 검토하여 판단한다. 또한 원래 목적과 합리적인 연관성이 있고 예측이 가능해야 한다.
  - 예를 들어, 직원정보를 효율적으로 관리하기 위해 중앙 집중식 DB로 처리하거나, 신용 대출을 위해 수집한 정보를 그 후속적인 채권 추심 목적으로도 이용이 가능하다. 이때 원래의 목적과의 관련성에 대한 합리성을 입증을 할 수 있어야 하며, 신청인은 이에 대한 명확한 증빙을 위해 개인정보 수집 시 고지했던 내용과 동의 받았던 기록을 보관하는 것이 바람직하다.

- 개인정보 수집 시 고지하거나 동의 받은 목적 또는 이와 관련된 목적 이외로 개인정보를 이용하는 경우 정보주체의 동의 또는 법령 근거 등 반드시 해당 이용에 대한 명확한 근거가 있어야 한다. 따라서 목적 외 이용의 경우를 나열하고 각 사례별로 근거를 명확히 수립하여야 하며, 필요 시 개인정보 처리방침 등에 공개하여야 한다.

- 정보주체의 동의를 받을 때에는 동의 내용을 명확하고 알기 쉬운 언어와 방법으로 고지하고, 정보주체가 동의 의사를 명시적으로 표시할 수 있는 수단을 제공하는 등 명시적 동의(expressed consent)를 받아야 한다. 정보주체의 동의 획득에 대한 입증 책임은 신청인에게 있다.

증적 자료

- 개인정보 목적 외 이용 제한에 관련한 내부 개인정보 정책/지침
- 개인정보 처리 관한 정보주체 동의 획득 절차 및 관련 내부 정책/지침
- 개인정보 수집 시 고지한 개인정보 수집·이용 목적
- 개인정보 처리방침
- 개인정보흐름도/흐름표

결함 사례

- 물품배송 안내를 목적으로 수집한 휴대폰번호로 별도의 동의 없이 할인 상품 안내 문자메시지를 보낸 경우
- 원래의 수집 목적과 관련된 목적으로써 개인정보를 처리하고 있다고 설명하나, 그 관련성을 합리적으로 입증하지 못하는 경우
- 개인정보 수집 시 고지한 목적 외로 개인정보를 이용하기 위해 정보주체의 동의를 받고 있으나, 동의 표시 란에 기본 값으로 동의 표시가 된(☑) 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 정보주체의 동의를 받거나 법령상 의무 준수를 위해 불가피한 경우 등 개인정보를 수집할 수 있는 근거 규정을 정하였으며, 그 수집 목적의 범위에 한하여 개인정보를 이용하도록 명시하였다. 이에 더해 당초 '수집 목적과 합리적으로 관련된 범위'에 대해서는 정보주체에게 불이익이 발생하는 지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 정보주체의 추가적인 동의 없이 개인정보를 이용할 수 있도록 하였다.

- 그러나 정보주체로부터 별도의 동의를 받는 등 다음의 경우에는 개인정보를 수집한 목적 외로 이용하거나 제3자에게 제공이 가능하다. 이 중 목적 외 이용을 위해 정보주체에게 추가적으로 동의를 받을 때에는 개인정보 수집 동의와 동일한 방법으로 필요 사항을 고지하고 동의를 받도록 했다.

개인정보 보호법 : 정보주체의 동의 없이 개인정보 이용 또는 제공이 가능한 경우

개인정보 보호법 제18조	개인정보 보호법 제39조의3
1. 정보주체로부터 별도의 동의를 받은 경우 2. 다른 법률에 특별한 규정이 있는 경우 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우 5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 8. 법원의 재판업무 수행을 위하여 필요한 경우 9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우 (5~9번의 경우 공공기관만 해당)	1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)

관련 ISMS-P 인증기준

- 3.2.5 (개인정보 목적 외 이용 및 제공) 개인정보는 수집 시의 정보주체(이용자)에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체(이용자)의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.

3.2 제공/위탁

3.2.1 제공 여부

10. 수집한 개인정보를 다른 개인정보처리자에게 제공하는 경우 제공과 관련한 상세 내용을 기술하시오.

3.2.2 위탁 여부

11. 수집한 개인정보를 개인정보 수탁사에게 위탁하여 처리하는 경우 위탁과 관련한 상세 내용을 기술하시오.

3.2.3 목적 내 제공/위탁

12. 개인정보를 제3자에게 제공 또는 위탁하여 처리하는 경우, 이러한 처리가 개인정보의 원래의 수집 목적 달성 또는 이와 관련된 목적을 위한 것이라면, 그 근거를 기술하시오.

3.2.4 목적 외 제공/위탁

13. 개인정보의 원래의 수집 목적 달성 또는 이와 관련된 목적 범위 외 개인정보를 제3자 제공하거나 위탁하여 처리하는 경우, 그 근거를 기술하시오.

a) 개인의 명시적 동의
b) 개인이 요구한 서비스 또는 제품의 제공을 위해 필요한 경우
c) 다른 법률에 근거한 경우

주요 확인사항

■ 제휴, 연계 서비스 등을 통해 개인정보를 제3자에게 제공하는가?

- 개인정보 제공 목적, 절차 등이 내부 정책/지침 등에 반영되어 있는가?
- 개인정보 수집 시 개인정보 제3자 제공(또는 제공 가능성)에 관한 사항을 고지하는가?
- 수집 시 고지한 개인정보 수집·이용 목적 또는 이와 관련된 목적으로 개인정보를 제3자에게 제공 하는가? 이외 다른 목적으로 제공하는 경우는 어떤 경우이며 그 근거는 무엇인가?
- 개인정보 제공 목적 별 제공 받는 자, 제공하는 개인정보 항목 등을 식별하여 관리하는가?
- 제3자 제공 시 정보주체에 고지 또는 동의를 받는 경우 어떤 방법으로 고지 또는 동의 받는가?

■ 개인정보 처리 업무를 제3자에게 위탁하여 처리하는가?

- 업무 위탁 목적, 절차 등이 내부 정책/지침 등에 반영되어 있는가?
- 개인정보 수집 시 업무 위탁에 관한 사항을 고지하는가?
- 수집 시 고지한 개인정보 수집·이용 목적 또는 이와 관련된 목적으로 개인정보 처리를 위탁하는가? 이외 다른 목적으로 위탁하는 경우는 어떤 경우이며 그 근거는 무엇인가?
- 업무 위탁 목적 별 위탁받는 자, 위탁하는 개인정보 항목(또는 유형) 등을 식별하여 관리하는가?
- 개인정보 위탁 시 정보주체에 어떤 방법으로 고지하는가?

- (위탁/제공 정책 수립) 개인정보 처리 업무를 위탁하여 처리하거나 업무 제휴 등을 목적으로 제3자 제공하는 경우, 내부 정책이나 지침에 이러한 처리에 대한 원칙, 절차 등을 수립하고 이에 따라 처리해야 한다. 또한 개인정보 처리 목적별 개인정보의 이용 또는 제공·위탁되는 현황을 개인정보 흐름도에 반영하여 체계적인 관리가 되도록 해야 한다.
  - 업무 위탁 현황: 위탁 목적, 위탁 업체명, 위탁하는 개인정보 항목 등
  - 제3자 제공 현황: 제공 목적, 제공받는 자, 제공하는 개인정보 항목 등
- (목적 내 위탁/제공) 개인정보 처리 위탁 또는 제3자 제공이 개인정보 수집 시 고지한 수집·이용 목적 범위 내 이루어지는 경우 이를 위한 추가적인 절차가 필요하지 않다. 원래의 목적에 부가된

목적 등 관련성이 높은 목적을 위한 위탁이나 제공도 가능하다. 예를 들어 직원의 급여 관리, 지급 업무 또는 상품 배송 업무를 위탁하는 경우 별도의 절차 없이 가능하다.

- (목적 외 위탁/제공) 그러나 원래의 수집·이용 목적과 다른 목적으로 개인정보를 제3자에 위탁처리하거나 제공하려는 경우 다음의 경우로 제한된다.
  - 정보주체로부터 명시적 동의를 받은 경우
  - 정보주체가 요구한 서비스 또는 제품의 제공을 위해 필요한 경우
  - 다른 법률에 의한 경우

- (명시적 동의) 정보주체의 동의를 받을 때에는 동의 내용을 명확하고 알기 쉬운 언어와 방법으로 고지하고, 정보주체가 동의 의사를 명시적으로 표시할 수 있는 수단을 제공하는 등 명시적 동의(expressed consent)를 받아야 한다. 정보주체의 동의 획득에 대한 입증 책임은 신청인에게 있다.

증적 자료

- 개인정보 처리 위탁 및 제3자 제공에 대한 내부 개인정보 정책/지침
- 개인정보 처리 관한 정보주체 동의 획득 절차 및 관련 내부 정책/지침
- 개인정보 수집 시 고지한 개인정보 위탁 및 제3자 제공에 관한 사항
- 개인정보 처리방침
- 개인정보흐름도/흐름표

결함 사례

- 개인정보 처리방침에 수탁업체 이름을 공개하고 있으나 지속적으로 위수탁 현황을 갱신하지 않아 최근 계약한 수탁업체에 관한 정보가 누락된 경우
- 개인정보처리자가 고객 만족도 조사를 위해 타 공공기관에게 개인정보를 제공하고 있었으나 이용자의 동의나 법적 근거 등이 없는 경우
- 개인정보 처리 업무를 외부 업체에 위탁하여 처리하고 있으나, 이에 대해 개인정보 수집 시 고지를 하거나 개인정보 처리방침에 공개하지 않는 경우

개인정보 보호법과 비교

- 개인정보 보호법은 개인정보의 수집·이용과 업무의 위탁 처리 및 제3자 제공을 구분하여 필요한 조치 사항을 규정하고 있다. 원칙적으로 일부 예외의 경우를 제외하고 개인정보 수집·이용에 대한 정보주체의 사전 동의가 필요하며, 이후 이를 제3자에게 제공하려는 경우에도 제공 목적과 관계없이 별도 동의가 필요하다. 위탁 처리의 경우에는 동의 절차 없이 해당 사항을 개인정보 처리방침에 공개하거나 개별 고지하여야 한다.

- 개인정보 보호법에 따라 개인정보를 제3자에게 제공할 수 있는 경우는 다음과 같다.

개인정보 제3자 제공이 가능한 경우(개인정보 보호법 제17조)

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

- 개인정보 제3자 제공에 대한 동의를 받을 때에는 다음을 포함한 사항을 알리고 동의 받도록 하여 엄격하게 규율하고 있다.

  – 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제17조(개인정보의 제공)
- 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)
- 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
- 개인정보 보호법 시행령 제28조(개인정보의 처리 업무 위탁 시 조치)

관련 ISMS-P 인증기준

- 3.3.1 (개인정보 제3자 제공) 개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체(이용자)의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.

- 3.3.2 (업무 위탁에 따른 정보주체 고지) 개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁사 등 관련사항을 정보주체(이용자)에게 알려야 하며, 필요한 경우 동의를 받아야 한다.

- 3.2.5 (개인정보 목적 외 이용 및 제공) 개인정보는 수집 시의 정보주체(이용자)에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체(이용자)의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.

3.3 자료 제출 요구 대응

3.3.1 자료 제출 요구 대응

45. 사법기관 또는 정부기관의 개인정보 제공 요청(소환장, 영장, 명령 등)에 대응하기 위한 절차가 마련되어야 한다.

주요 확인사항

■ 개인정보의 제공을 요구하는 법원 또는 정부기관 등의 소환장, 영장 또는 명령 시 개인정보를 제공하는가?

■ 위와 같은 요구에 대응하는 절차를 마련하고 있는가?

- 법집행기관 또는 사법기관, 수사기관 등으로부터 해당 기관의 업무를 수행하기 위해 신청인이 보유하고 있는 개인정보를 요구하는 경우 적법한 절차에 따라 제공해야 한다.
- CBPR의 개인정보 보호 원칙에 따라 개인정보처리자는 원칙적으로 정보주체의 개인정보의 수집·이용 목적 이외의 용도로는 이용하거나 제3자에게 제공할 수 없다. 다만 정보주체의 동의가 있거나 관련 법령 등에 따른 경우에는 제3자 제공 등이 가능하다.
- 따라서 제공에 대한 법적 근거, 정식 공문(압수수색영장 등) 요청, 요청 기관의 담당자 확인, 최소 정보 제공 원칙 등의 절차와 원칙이 포함된 정책을 마련하여 운영해야 한다. 또한 개인정보 제공 과정에서 정보가 유·노출되지 않도록 안전한 절차와 방법을 활용하고 개인정보 제공 내역을 기록하여 일정 기간 보관한다.

제공 시 안전한 절차	제공 시 기록에 포함할 사항
• 제3자와 제공과 관련된 내부 승인절차 • 전송 및 전달 과정의 암호화 • 접근통제 등 안전성 확보조치 적용 • 제공 정보에 대한 기록 보존	• 제공받는 자, 제공한 일시 • 제공된 개인정보(개인정보 항목 등) • 근거 법령 • 제공 방법(시스템 연계, 이메일 전송 등)

증적 자료

- 자료(개인정보) 제출 요청 공문 및 개인정보 제공 내역, 대장
- 자료(개인정보) 제출 요청 대응 매뉴얼

결함 사례

- 사법기관이 개인정보 제출 요구에 대한 근거 법률 등을 명시하지 않고 이메일 형식으로 필요한 자료 등을 요청하였으나 별도 검토 과정 없이 자료를 제공한 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법에서는 정보주체의 동의 없이 제3자에게 개인정보를 제공하는 것이 원칙적으로 제한되나, ▲ 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, ▲ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 등에는, (정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 없는 경우에 한하여) 개인정보를 제공할 수 있다고 규정하고 있다.

- 관련 법령의 예시로, 통신비밀보호법에서는 검사 또는 사법경찰관이 수사 또는 형의 집행을 위하여 전기통신사업자에게 통신사실 확인자료 제출을 요청할 수 있으며, 전기통신일시, 가입자 번호 등 요청가능 자료의 범위를 정하고 있다. 자료 요청 시에도 요청사유 등에 대해 관할 지방법원으로부터 허가를 받아서 해당 전기통신사업자에게 요구하도록 절차를 규정하고 있다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제17조(개인정보의 제공)
- 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)

• 관련 ISMS-P 인증기준 •

- 3.2.5 (개인정보 목적 외 이용 및 제공) 개인정보는 수집 시의 정보주체(이용자)에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체(이용자)의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.

- 3.3.1 (개인정보 제3자 제공) 개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체(이용자)의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.

4. 정보주체 권리

4. 정보주체 권리

- 4.1 열람권
- 4.2 정정·삭제권
- 4.3 선택권
- 4.4 민원제기

4.1 열람권

4.1.1 개인정보 보유 여부 확인권

36. 정보주체의 요청 시 신청인이 해당인의 개인정보의 처리 여부에 대해 확인해주어야 한다.

4.1.2 열람권

37. 정보주체의 개인정보 열람 요청 시, 다음의 요건에 따라 열람 처리를 하여야 한다.

1) 정보주체의 본인확인
2) 처리 기한을 정하고 정해진 기한 내 처리
3) 이해하기(읽기) 쉬운 개인정보 파일 형식으로 제공
4) 일반적인 통신/전송 방법(이메일 등) 으로 제공
5) 열람처리에 대한 비용을 청구하는 경우, 청구 사유 및 비용산정 근거 제시

주요 확인사항

- ■ 정보주체 요청 시 해당 정보주체의 개인정보 보유 여부를 확인하고 열람·정정 및 삭제하는 절차와 방법을 마련하고 있는가?
- ■ 정보주체가 이러한 개인정보 열람·정정 및 삭제에 대한 권리 및 행사 방법을 명확하게 인지할 수 있도록 고지하는가?
- ■ 정보주체의 요청에 대한 처리 시에는 정보주체의 신원을 확인하는 절차가 있는가?
- ■ 개인정보 열람 요청에 대한 처리 시에는 다음의 사항이 고려되었는가?
  - 보편적으로 쉽게 판독 가능한 형식으로 제공
  - 일반적으로 쉽게 이용할 수 있는 소통 수단(언어, 전송수단)으로 제공
- ■ 정보주체가 열람 가능한 개인정보의 범위는 무엇인가?
- ■ 열람 처리에 비용을 정보주체에게 청구하는 경우 비용 산정 근거나 기준을 마련하였는가?
- ■ 정보주체의 요청에 대한 합리적인 처리 기간을 정하고 기간 내에 처리하는가?
- ■ 정보주체의 요청에 대한 조치 완료 후 조치 결과에 대해 회신하는 절차가 있는가?
- ■ 정보주체의 요청을 거부하는 경우, 정보주체에 거부 사유를 설명하고 이의 제기 등의 방법을 안내하는 절차가 있는가?

- 정보주체는 개인정보처리자가 자신의 개인정보를 처리하고 있는지 여부 확인, 그리고 처리하는 경우 이에 대해 열람을 요청할 권리가 있다. 신청인은 정보주체가 이러한 권리를 명확히 인지하고 원활히 행사할 수 있도록 절차를 마련하고 조치해야 한다. ☞ [2.2.1 개인정보 처리방침 공개] 참고

- (본인 확인) 먼저, 개인정보 보유 여부 확인, 열람 등을 요청하는 개인이 정보주체인지 여부를 확인하여 타인에 의한 불법적인 접근을 방지해야 한다. 신원 확인의 방법은 다음과 같이 신청인이 보유하고 있는 기존의 정보를 활용하는 등 정보주체가 쉽게 이행할 수 있는 방법을 선택하여야 하며, 복잡한 절차를 요구하거나 신원확인을 목적으로 과도하게 추가 정보를 수집하여 열람권 행사를 어렵게 해서는 안 된다.
  - (온라인) ID/PW 인증, 이메일 인증, 휴대폰 인증, 아이핀 인증 등
  - (오프라인) 신분증, 자동차면허등록증 등 확인
  - (아동) 정보주체가 만14세 미만인 경우에는 법정대리인의 신분 확인 및 동의

- (기한 내 처리) 신청인은 열람 요청에 대한 합리적인 처리 기한*을 정하고 기한 내 처리하여야 한다. 기한 내 처리를 못하는 정당한 사유가 있는 경우에는 기한 만료 전에 그 사유와 함께 처리 경과 등에 대해 정보주체에게 통지하고 그 사유가 소멸하는 즉시 조치를 이행하여야 한다.

  * CBPR은 처리 기한을 특정하지 않고 있으나 국내 개인정보 보호법에 규정하는 처리 기한(열람 요구 후 10일 이내)을 참고하여 정할 수 있다.

- (열람 방법) 개인정보 열람 요청 및 열람의 방법은 정보주체와 소통했던 방법 또는 이메일, 홈페이지 또는 전화, 서면 등 일반적으로 쉽게 접근할 수 있는 매체여야 하며, 개인정보의 형식 또한 구조화된 형식(서면, 전자적 파일 등)과 내용으로 일반인이 쉽게 판독할 수 있어야 한다. 특히 내국인뿐만 아니라 해외 이용자들도 이용하는 글로벌 서비스를 제공하는 경우 이들에게도 통용되는 언어를 사용해야 한다.

- (열람 항목) 정보주체는 다음의 사항에 대한 열람을 요청할 수 있다. 이때 정보주체 등으로부터 수집된 개인정보 이외에도 신청인이 생성하거나(거래내역 등), 자동으로 생성된 개인정보(쿠키 등)도 열람 대상에 포함된다.
  - 개인정보 이용 목적별 개인정보 항목(또는 유형)
  - 제3자 제공(또는 제공 예정) 시 제공 목적 및 제공받는 자, 제공하는 개인정보 항목(또는 유형) 등
- (비용 청구) 신청인은 개인정보 열람을 처리하는 과정에서 비용이 발생하는 경우 그 실비에 대해 정보주체에 부과할 수 있다. 이때 신청인은 비용 산정 근거가 과도하지 않고 합리적임을 입증해야 한다.

- (거부) 다음의 경우에는 정보주체의 개인정보 열람, 정정 요청을 거부할 수 있다.
  - **과도한 요청**: 지나치게 반복적이거나 성가신(vexatious) 요청 등 정보주체의 권리 보호 효과에 비해 과도한 비용과 처리 작업이 요구되는 경우
  - **기업 영업비밀 등 침해**: 신청인의 영업 비밀이나 정보보안, 또는 다른 법적인 권리에 침해가 되는 경우
  - **타인의 권리 침해**: 정보주체의 권리 행사로 인해 타인의 개인정보나 권리가 침해될 가능성이 있는 경우

증적 자료

- 개인정보 열람권과 관련한 내부 정책/지침
- 개인정보 처리방침
- 정보주체의 본인 확인 절차, 관련 양식
- 개인정보 열람 요청에 대한 접수, 처리 등 관련 절차, 양식
- 개인정보 열람 요구에 대한 처리/거부 내역
- 열람 비용을 부과하는 경우 비용 산정 근거

결함 사례

- 정보주체 본인 또는 정당한 대리인이 맞는지에 대한 본인확인 절차 없이 열람 통지가 이루어지는 경우
- 개인정보의 열람 요구 처리를 정당한 사유의 통지 없이 지체하고 이에 대해 처리 기한 내 회신하지 않는 경우
- 개인정보 열람 처리에 대한 비용 청구 시, 산정 근거가 합리적이거나 정당하지 않는 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 정보주체의 개인정보 열람, 정정, 삭제의 권리를 보장하여 CBPR의 동 항목과 유사하며, 이에 더해 세부 이행 규정이 구체적이다. 또한 정보주체로부터 직접 수집한 개인정보뿐만 아니라 정보주체 이외로부터 수집한 개인정보에 대해서도 이러한 권리가 적용된다. CBPR과 같이 열람 등을 요구하는 정보주체의 본인 확인 절차에 대한 명시적인 규정은 없다. 또한 정보주체의 요청에 대한 거부는 법률에 따라 열람이 금지되는 경우나 타인의 권리 침해 등으로 엄격하게 제한되어, 기업의 합리적인 기업 활동에 저해되는 요소들을 함께 고려한 CBPR과 차이가 있다.

- 이 법에 따라 개인정보처리자는 정보주체의 개인정보 열람 요구 시 ▲ 개인정보의 항목 및 내용, ▲ 개인정보의 수집·이용의 목적, ▲ 개인정보 보유 및 이용 기간, ▲ 개인정보의 제3자 제공 현황, ▲ 개인정보 처리에 동의한 사실 및 내용 등 열람 항목을 구체적으로 명시했다. 또한 정보주체가 열람을 요구하는 방법과 열람하는 방법을 개인정보의 수집 방법과 절차에 비해 어렵지 않게 마련하도록 했다. 개인정보 보호법은 열람 처리 기한을 요청 받은 후 10일 이내로 규정하고, 기한 내 처리하지 못하는 정당한 사유가 있는 경우, 정보주체에게 그 사유를 알리고 열람을 연기할 수 있다. 또한 열람·정정·삭제 조치에 대한 결과를 정보주체에게 알릴 때 개인정보보호위원회 고시에서 정한 통지서로 알리도록 하였다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)
- 개인정보 보호법 제35조(개인정보의 열람)
- 개인정보 보호법 제38조(권리행사의 방법 및 절차)
- 개인정보 보호법 제39조의7(이용자의 권리 등에 대한 특례)
- 개인정보 보호법 시행령 제41조(개인정보의 열람절차 등)
- 개인정보 보호법 시행령 제47조(수수료 등의 금액 등)
- 개인정보 보호법 시행령 제46조(정보주체 또는 대리인의 확인)

• 관련 ISMS-P 인증기준 •

- 3.5.2 (정보주체 권리보장) 정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.

4.2 정정·삭제권

4.2.1 정정·완성·삭제권

38. 정보주체의 요청 시, 다음의 요건에 따라 개인정보를 정정하거나 완성, 삭제하는 등의 처리를 해야 한다.

1) 정정/완성/삭제 요청 절차를 명확하게 표시
2) 처리 기한을 정하고, 정해진 기한 내 처리
3) 처리 사실 통지
4) 정보주체 요구에 대해 처리 거부 시, 거부 사유 및 거부에 대한 이의 제기할 수 있는 연락처 제공

주요 확인사항

- ■ 정보주체가 개인정보 정정, 완성 및 삭제에 대한 권리 및 신청 방법을 명확하게 인지할 수 있도록 안내하고 있는가?
- ■ 정보주체의 이러한 요청에 대한 처리 절차를 마련하고 있는가?
- ■ 정보주체의 요청에 대한 처리 기한을 정하고 기한 내 처리하는가?
- ■ 정보주체의 요청에 대한 처리 완료 후 처리 결과를 회신하는가?
- ■ 정보주체의 요청을 거부하는 경우, 정보주체에 거부 사유를 설명하고 이의 제기 등의 방법을 안내하는 절차가 있는가?

- (정정·완성·삭제권) 정보주체는 자신의 개인정보에 대해 열람하고 정확하지 않거나 보완이 필요한 정보에 대해 정정, 완성 또는 삭제를 요청할 수 있는 권리가 있으며, 신청인은 정보주체의 요청에 대한 처리 절차를 마련하고 이를 지체 없이 조치해야 한다. 이때 신청인은 해당 정보가 부정확한지 여부를 확인하기 위해 필요한 자료를 정보주체에게 요구할 수 있다.

- (처리결과 통지) 정보주체의 요청에 따른 처리 후 처리 결과를 정보주체에게 통지해야 한다. 개인정보 정정, 삭제 등 변경된 개인정보 파일의 사본을 전송하거나 처리 완료 사실을 서면, 이메일, 전화 등의 방법으로 통지한다.

- 그 외 정보주체의 개인정보 정정, 삭제 권리 안내, 요청 절차 및 거부 등의 사항에 대해서는 【CBPR 자가 평가 질문37】에 따른 내용을 참조한다.

증적 자료

- 개인정보 정정, 삭제권에 대한 내부 정책/지침
- 개인정보 처리방침
- 개인정보 정정, 삭제 요청에 대한 접수, 처리 등 관련 절차, 양식
- 개인정보 정정, 삭제 요청에 대한 처리/거부 내역

결함 사례

- 온라인 회원 가입을 통해 개인정보를 수집하였으나, 회원 정보 수정 또는 삭제를 위해서는 서식 양식을 제출해야 하는 경우
- 개인정보의 정정, 삭제 처리 후 처리 결과에 대한 통지 절차가 없어 정보주체가 처리 사실을 인지하기 어려운 경우
- 개인정보 삭제 요청을 거부하였으나 그 사유가 합리적이거나 정당하지 않는 경우

개인정보 보호법과 비교

- 개인정보 보호법은 정보주체의 요구 시 10일 이내 개 인정보의 정정, 삭제 등의 조치를 한 후 그 결과에 대해 정보주체에게 알리도록 규정했다. 다만 다른 법률에 따라 보존의 의무가 있는 개인정보의 경우에는 삭제를 요구할 수 없다.
- 이 밖에 일반적인 정보주체의 권리 행사 방법, 절차 등에 관한 개인정보 보호법의 내용은 [4.1.2 열람권]의 내용을 참고한다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제36조(개인정보의 정정·삭제)
- 개인정보 보호법 제38조(권리행사의 방법 및 절차)
- 개인정보 보호법 시행령 제43조(개인정보의 정정·삭제 등)

관련 ISMS-P 인증기준

- 3.5.2 (정보주체 권리보장) 정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.

4.3 선택권

4.3.1 수집 제한

> 14. 개인정보 수집에 대해 정보주체가 선택할 수 있는 체계를 마련하여야 한다.

4.3.2 이용 제한

> 15. 개인정보 이용에 대해 정보주체가 선택할 수 있는 체계를 마련하여야 한다.

4.3.3 제3자 제공 제한

> 16. 개인정보 제3자 제공에 대해 정보주체가 선택할 수 있는 체계를 마련하여야 한다.

주요 확인사항

- ■ 개인정보 수집에 대해 정보주체가 제한할 수 있는 체계를 마련하였는가?
- ■ 개인정보 이용에 대해 정보주체가 제한할 수 있는 체계를 마련하였는가?
- ■ 개인정보 제3자 제공에 대해 정보주체가 제한할 수 있는 체계를 마련하였는가?
- ■ 정보주체가 개인정보 처리를 제한할 수 있는 시점은 언제인가?
- ■ 개인정보 처리 유형이나 목적별로 처리를 제한할 수 있는 선택권이 있는가?
- ■ 정보주체의 개인정보 수집·이용 또는 제공에 대한 제한 요청으로 인한 불이익이 있는가?

- 선택권은 신청인이 개인정보 수집·이용 또는 제공에 대해 정보주체가 명확히 인지하게 하고 원하는 경우 이를 제한하거나 거부(opt-out)할 수 있도록 하는 권리로, 우리 개인정보 보호법에서 정보주체로부터 개인정보 처리에 대한 사전 동의(opt-in)를 받도록 하는 원칙과 구분된다.

- 일반적으로 개인정보 처리가 이루어지기 전에 정보주체가 처리 제한 여부를 선택할 수 있어야 하며, 따라서 개인정보 수집 후 이용 또는 제3자 제공이 바로 이어지는 경우 수집 시점에 선택권이 주어져야

한다. 그러나 수집 이후 이용 또는 제공이 결정되거나 원래의 수집 목적과 다른 목적으로 이용 또는 제공되는 경우에는, 수집이 된 이후에 그러나 해당 처리가 이루어지기 전에 제한할 수 있는 절차가 마련되어야 한다.

※ 원래의 수집 목적과 다른 목적으로 이용하거나 제공하려는 경우에는 선택권과는 별도로 정보주체의 명시적 동의나 법률의 근거 등 처리에 대한 근거가 있어야 처리가 가능하다.

- 신청인은 정보주체의 요청에 따라 개인정보 처리의 일부 또는 전부를 중지하거나 파기 등의 조치를 하도록 체계와 절차를 마련해야 한다. 즉, 정보주체의 요청 시 개인정보의 일부 또는 전체를 수집·이용하거나 제3자에 제공하는 것을 제한해야 한다. 혹은 특정 목적으로 개인정보를 이용 또는 제공하지 않아야 한다. 이를 위해 신청인은 합리적인 범위 내에서 개인정보 처리 목적별, 처리 형태별(수집, 이용, 제공) 처리되는 개인정보 항목을 구분하고 각각에 대한 선택을 할 수 있도록 구현해야 한다.
  - 신청인은 기본적인 서비스 제공에 필요한 개인정보 이외 추가 서비스 등에 필요한 개인정보 수집·이용을 거부한다고 해서 해당 기본적인 서비스 제공을 거부하는 등 정보주체가 요청한 사항과 관련 없는 서비스나 상품의 제공을 거부해서는 안 된다.

적용 예외

- 다음의 경우에는 정보주체에게 개인정보 처리에 대한 선택권을 보장하는 것이 어렵다고 인정되거나 반드시 필요하지는 않다.
  - **(암묵적 동의로 간주되는 경우)** 정보주체가 개인정보 수집·이용·제공 사실, 목적 등을 명확하게 인지/예측이 가능하여 이러한 개인정보 처리에 대해 암묵적으로 동의한 것으로 간주될 수 있는 상황의 경우(ex: 업무적 목적으로 명함 제공)
  - **(공개적으로 이용 가능한 정보의 수집)** 공개 명부 등 공개적으로 이용 가능한 정보를 그 공개된 목적으로 수집·이용하는 경우
  - **(제3자로부터 받은 정보)** 제3자로부터 개인정보를 제공받은 경우 수집에 대한 선택권을 제공할 필요는 없음
  - **(기술적 불가능)** 잠재적 이용자의 초기 접속 등 전자 기술적으로 자동 수집되는 정보(쿠키 등)의 경우. 이 경우에도 사후에, 그러나 가능한 빠른 시일 내 선택권을 제공해야 함
  - **(법집행 기관에 제공되는 정보)** 법집행 기관이 수사 목적으로 요청한 정보를 제공하는 경우로써, 이에 대한 고지가 수사에 방해될 것으로 예상되는 경우
  - **(법적 절차에 따라 제공되는 정보)** 소송 절차에 의한 요청 등 법적 절차, 양식에 의해 제공되는 개인정보의 경우
  - **(합법적 조사 목적)** 법령, 규약 등의 위반에 대한 내/외부 조사와 관련된 목적으로 개인정보 처리가 합리적으로 필요하고, 이에 대해 고지할 경우 정보 정확성이나 활용성이 침해될 것으로 예상되는 경우
  - (**긴급 상황**) 개인의 생명, 건강 또는 안전을 위협하는 긴급 상황에서 처리하는 개인정보의 경우

증적 자료

- 정보주체의 선택권과 관련한 내부 개인정보 정책/지침
- 개인정보 수집 시 고지와 관련한 내부 개인정보 정책/지침
- 정보주체의 선택권 행사 절차가 포함된 온라인화면, 서면 가입 신청서 등

결함 사례

- 원래의 수집 목적과 다른 목적으로 개인정보를 이용하거나 제3자 제공하였으나, 이러한 처리 이후에 정보주체에게 선택권을 제공한 경우
- 다수의 제3자에게 다른 목적으로 개인정보를 제공하고 있으나, 각각에 대한 선택권이 구분되어 제공되지 않고 일괄적으로 제공되는 경우
- 맞춤형 마케팅을 위한 쿠키 정보 수집·이용을 거부하였으나, 이와 관련 없는 다른 서비스 이용이 포괄적으로 제한되는 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 다른 법률에 의한 경우 등 특별한 경우를 제외하고는 개인정보 수집 등 처리를 위해서는 정보주체의 사전 동의가 필요하다. 정보주체로부터 동의를 받을 때에는 동의 거부권 및 거부 시의 불이익을 포함한 처리에 관한 주요 사항을 고지하야야 한다. 또한 서비스 제공에 필수적인 사항과 선택적인 사항에 대한 동의를 구분하여 선택적인 항목의 경우 동의하지 않아도 기본 서비스 제공에 제한이 없도록 규정하고 있다. 이때 개인정보처리자는 필수 수집 정보가 서비스 제공을 위한 최소한의 개인정보임을 입증할 책임이 있다.

- 정보주체는 개인정보처리자에게 개인정보처리에 대한 동의를 철회하거나 처리 정지를 요구할 권리가 있다. 개인정보처리자는 이러한 정보주체의 요구에 따라 다음의 예외 사항을 제외하고는 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 하며, 정보주체의 요구를 거절하는 경우에는 거절 사유에 대해 지체 없이 통지해야 한다. 정보주체의 요구에 따라 처리가 정지되거나 동의 철회된 개인정보에 대해서는 지체 없이 파기 등 필요한 조치를 하여야 한다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제22조(동의를 받는 방법)
- 개인정보 보호법 제37조(개인정보의 처리정지 등)
- 개인정보 보호법 제39조의7(이용자의 권리 등에 대한 특례)

관련 ISMS-P 인증기준

- 3.1.1 (개인정보 수집 제한) 개인정보는 서비스 제공을 위하여 필요한 최소한의 정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다.
- 3.5.2. (정보주체 권리보장) 정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.

4.3.4 선택권 행사

19. 정보주체가 선택권을 쉽고 (필요 시) 합리적인 비용으로 행사할 수 있도록 방법을 마련해야 한다.

4.3.5 선택권 조치

20. 정보주체가 선택권 행사 시, 이를 효과적이고 신속하게 조치하기 위한 방법과 절차를 마련해야 한다.

주요 확인사항

- ■ 정보주체가 개인정보 수집·이용·제공 제한에 대한 선택권을 실제로 행사하기 쉽고 합리적인 방법으로 구현하고 있는가?
- ■ 정보주체에게 선택권 제공에 대한 비용을 청구한다면 이러한 비용이 합리적인 비용임을 입증할 수 있는가?
- ■ 정보주체의 개인정보 처리 제한 요청을 접수하고 조치하기 위한 절차가 마련되었는가?
- ■ 정보주체의 요청 처리 담당자를 지정하고 합리적인 처리 기한을 정하였는가?

- 신청인은 정보주체가 선택권을 쉽게 행사할 수 있도록 방법과 절차를 구현해야 한다. 서비스 형태를 고려하여 홈페이지/모바일 앱 내 메뉴 구성 또는 이메일, 전화 요청 등 일반적으로 많이 사용되는 매체나 기술적 방법 등을 활용하여 정보주체가 과도한 노력과 비용을 들이지 않고 행사할 수 있도록 해야 한다. 다만 신청인은 선택권 처리에 소요되는 경비(해당 건 처리에만 드는 비용 기준)에 대해 합리적인 수준에서 정보주체에게 비용을 청구할 수 있다.

- 신청인은 이러한 정보주체의 요청 사항을 신속하고 효율적으로 조치하기 위한 방법과 절차를 마련해야 한다. 정보주체의 요청 사항을 접수, 처리하는 담당 부서를 지정하고, 이를 개인정보 처리 시스템에 반영하거나 관련 부서에 전달하는 등의 업무 절차가 수립되어야 한다. 개인정보 처리를 위탁하여 처리하는 경우에는 해당 수탁사에 이를 전달하여 변경 사항을 신속히 반영할 수 있도록 업무 절차가 마련되어야 한다.

- 신청인이 정보주체의 선택권에 대한 요청을 거부해야하는 합리적인 사유가 있는 경우 관련한 내부 개인정보 처리 지침이나 매뉴얼에 이를 명시하여야 하며, 거부 사유가 타당한지에 대한 입증 책임은 사업자에게 있다.

- 선택권 요청에 대한 조치는 신속히 이루어 질 수 있도록, 접수·처리·통지 등 처리 단계별 합리적인 처리 기간을 지정하고 해당 기한 내 처리해야 한다. 신청인은 정보주체에게 요청 사항에 대한 접수, 예상 처리 기간 및 처리 결과를 통지해야 한다. 또한 신청인이 합리적인 사유로 정보주체의 요청 사항을 이행하지 못하는 경우에는 해당 정보주체에게 그 사유를 알려야 한다.

증적 자료

- 선택권 행사와 관련된 홈페이지/모바일 앱 내 메뉴, 연락처 안내 화면 등
- 정보주체의 선택권 행사에 대한 조치 매뉴얼

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 정보주체가 언제든지 개인정보 수집·이용 및 제공에 대한 동의 철회 또는 처리 정지를 요청할 수 있도록 하고 이러한 요청 방법은 개인정보의 수집 방법보다 쉽게 하여야 한다고 규정하였다. 개인정보처리자는 정보주체의 요청에 대해 해당 요구 사항에 따라 지체 없이 개인정보의 일부 또는 전부에 대해 파기 등의 조치를 취해야 한다.

결함 사례

- 온라인 서비스 관련 제휴를 위한 개인정보 제3자 제공에 대해 정보주체에게 선택권을 제공하고 있으나, 선택권 행사를 위한 불가피한 방법이 아님에도 특정 어플리케이션을 설치하도록 하거나 우편이나 팩스로 신청하도록 한 경우
- 정보주체가 홈페이지에서 이메일 수신 거부를 요청하였으나, 요청 사항이 개인정보처리시스템에 즉각 반영되지 않아 거부의사를 밝힌 이후에도 이메일이 발송된 경우

관련 ISMS-P 인증기준

- 3.5.2 (정보주체 권리보장) 정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.

관련 법령

법령

- 개인정보 보호법 제37조(개인정보의 처리정지 등)
- 개인정보 보호법 제38조(권리행사의 방법 및 절차)
- 개인정보 보호법 제39조의7(이용자의 권리 등에 대한 특례)

4.4 민원제기

4.4.1 민원 처리 절차

41. 개인정보 관련 민원을 접수, 조사하고 대응하기 위한 절차를 마련해야 한다.

4.4.2 민원 처리 기한

42. 합리적인 개인정보 민원 처리 기한을 정하고 기한 내 처리해야 한다.

4.4.3 민원 처리

43. 개인정보 민원에 대한 처리 방안을 마련하여야 한다.

주요 확인사항

- 개인정보 관련 문의나 민원을 처리하는 부서 또는 담당자가 있는가?
- 정보주체가 개인정보 관련 민원을 신청할 수 있도록 절차를 마련하고 신청인의 홈페이지 등에 민원 접수 방법을 안내하고 있는가?
- 신청인은 민원 접수, 조사 및 조사 결과에 대한 처리 방안 등 민원 대응 절차 등에 대한 문서화된 매뉴얼이 있는가?
- 신청인은 민원 처리에 대한 합리적인 기한을 정하고 기한 내 처리하는가?
- 주요 민원 유형별 해결 방안 등 민원 처리 방안을 마련하였는가?

- 신청인은 민원인이 전화나 이메일 또는 홈페이지 등을 통해 개인정보와 관련한 문의나 불만 등 민원을 쉽게 신청할 수 있도록 민원 접수처를 마련하고, 홈페이지 내 개인정보 처리방침 등에 신청 방법을 안내하여야 한다.
- 신청인은 민원 처리부서 또는 담당자를 지정하고 접수된 민원에 대한 사실 관계 확인 등 조사, 그리고

조사 결과에 대한 합리적인 조치 방안 등 일련의 민원 처리에 대한 절차를 마련하고 이를 민원처리 매뉴얼 또는 내부 정책 등에 반영해야 한다. 본 매뉴얼 등에는 민원 처리 민원인의 개인정보를 보호하기 위한 조치가 포함되어야 한다.

- 민원 처리 시스템이나 문서는 담당자 이외 접근이 제한되어야 하며, 민원인의 정보를 포함한 민원처리 내용은 업무와 관련 없는 다른 제3자에게 공유하거나 누설해서는 안 된다.

증적 자료

- 개인정보 처리방침 등 민원 신청 방법에 대한 고지 화면/서면 신청서 등
- 민원 처리와 관련 홈페이지 내 메뉴, 모바일 채팅창, 서식지 등
- 개인정보 민원처리와 관련한 내부 정책/규정, 민원처리 매뉴얼
- 민원 처리 시스템

결함 사례

- 민원 처리 기한을 정하지 않고 합리적인 사유 없이 답변을 지연하는 경우
- 민원 처리 내역을 민원 담당자 이외 다른 직원이 접근 가능한 경우

개인정보 보호법과 비교

- 개인정보 보호법은 개인정보 보호책임자 지정을 의무로 규정하고, 책임자의 역할에 개인정보 처리와 관련한 불만의 처리 및 피해 구제를 포함하였다. 또한 개인정보 처리방침의 공개 시 개인정보 보호책임자의 성명 또는 개인정보 보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호를 표시하도록 규정하였다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개) ※ 제1항6호
- 개인정보 보호법 제31조(개인정보 보호책임자의 지정) ※ 제2항3호

관련 ISMS-P 인증기준

- 3.5.2 (정보주체 권리보장) 정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.

5. 무결성

5. 무결성

5.1 최신성 유지 | 5.2 최신정보 공유

5.1 최신성 유지

5.1.1 최신성 검증

21. 개인정보 이용 목적에 필요한 범위 내에서 개인정보의 정확하고 완전하며, 최신의 상태 여부를 검증하기 위한 조치를 취해야 한다.

5.1.2 최신화

22. 개인정보 이용 목적 내 필요한 범위 내에서 부정확, 불완전하거나 오래된 개인정보를 정정하기 위한 절차가 있어야 한다.

주요 확인사항

- 개인정보 처리 목적에 맞는 개인정보를 식별하고 개인정보의 정확성, 완전성, 최신성을 확인하는 절차를 마련하였는가?
- 정보의 최신성 등을 확인하는 체계는 처리하는 개인정보의 특성이나 정확하지 않는 정보의 사용으로 초래되는 위험 등을 고려하여 마련되었는가?
- 신청인은 개인정보가 정확, 완전 또는 최신의 상태가 아님을 확인 또는 의심되는 경우 이를 정정하기 위한 방법과 절차를 마련하고 있는가?

- (개요) 개인정보의 정확성, 완전성, 최신성을 유지하는 것은 정확하지 않는 개인정보 처리로 발생할 수 있는 정보주체 또는 개인정보처리자의 불이익을 방지하기 위해 필요하다. 예를 들어 멤버십 회원의 변경된 주소 정보가 회원 정보에 반영되지 않아 멤버십 카드 등의 우편물이 다른 곳으로 배송되거나, 금융 서비스 회원의 상향된 신용등급 정보가 반영되지 않아 금융 대출 등에 불이익을 겪을 수 있다.

- (검증) 신청인은 각 개인정보의 처리 목적에 필요한 개인정보를 식별하고 이의 정확성, 완전성, 최신성을 보장해야 한다. 주기적으로 회원을 대상으로 개인정보 이용 내역 통지나 개인정보 현행화 캠페인 등을 통해 정보주체가 스스로 자신의 개인정보를 확인하도록 하는 방법 등 개인정보 처리나 서비스 형태에 따라 적절한 방법을 마련한다.

- (주기) 최신화 주기나 시점은 업무 수행 주기나 개인정보의 특성, 또는 부정확한 정보사용 시 초래되는 위험 등을 고려하여 결정하는 것이 바람직하다. 예를 들어 VIP고객에게 매월 월간지를 발송하는 경우 매월 발송일 직전에 고객정보와 주소의 최신성을 확인하여 사용할 수 있다.

- (정정) 신청인은 보유하고 있는 개인정보가 부정확, 불완전 또는 오래됐다고 확인되거나 의심이 되는 경우 이를 신속히 정정할 수 있도록 처리 담당자를 지정하고, 관련 부서에 통지하는 절차 등을 마련해야 한다. 또는 정보주체가 직접 정보를 확인하고 수정할 수 있도록 홈페이지/모바일 앱 등에 관련 메뉴를 마련할 수 있다.

증적 자료

- 개인정보 정확성, 완전성, 최신성에 관련한 내부 개인정보 정책/지침
- 개인정보의 정확성, 완전성, 최신성 여부 확인 방법/절차
- 신청인 또는 정보주체가 개인정보를 정정할 수 있는 방법/절차

결함 사례

- 개인정보 DB에 정보 생성, 변경 등의 일시에 대한 정보가 없어서 회원정보의 최신성에 대한 확인이 어려운 경우
- 고객에게 서비스 이용 요금 통지서를 매월 우편 발송하고 있으나 개인정보 최신화 주기를 1년으로 설정하고 실시

개인정보 보호법과 비교

- 개인정보 보호법은 개인정보 처리 원칙 중의 하나로 개인정보 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성 보장을 규정하고 있다. 그러나 이러한 선언적인 원칙 외에 이의 구체적인 이행에 대한 규정은 별도로 명시되어 있지 않다.

- 다를 관계 법령으로, 개인의 신용정보를 규율하는 신용정보의 이용 및 보호에 관한 법률에서는 신용정보회사 등이 신용정보의 정확성과 최신성이 유지될 수 있도록 신용정보의 등록, 변경 및 관리 등을 하도록 하고 그 방법을 구체적으로 규정하고 있다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제3조(개인정보 보호 원칙)

관련 ISMS-P 인증기준

- 3.2.2 (개인정보 품질보장) 수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체(이용자)에게 관리절차를 제공하여야 한다.

5.2 최신정보 공유

5.2.1 수탁사에 통지

23. 부정확, 불완전하거나 오래된 개인정보가 이용 목적에 영향을 미치고, 수탁사에 정보가 이전된 후 정정이 이루어진 경우, 이러한 정정 사실을 수탁사에게 통지하는 체계를 마련해야 한다.

5.2.2 제3자에 통지

24. 부정확, 불완전하거나 오래된 개인정보가 이용 목적에 영향을 미치고, 정보의 제3자 제공 이후 정정이 이루어지는 경우, 이러한 정정 사실을 개인정보를 제공받은 자에게 통지하는 체계를 마련해야 한다.

5.2.3 수탁사로부터 통지

25. 수탁사가 처리하는 개인정보가 부정확, 불완전 또는 최신 상태가 아님을 인지할 때, 이를 수탁사로부터 통지받는 체계를 마련해야 한다.

주요 확인사항

- ■ 개인정보 정정 사항에 대해 관련 업무를 처리하는 수탁사에게 통지하고 수탁자가 이를 반영했는지에 대한 확인절차가 있는가?
- ■ 제3자에게 개인정보를 제공한 후 개인정보의 변경이 이루어진 경우 해당 제3자에게 변경 사실을 알리는 절차가 있는가?
- ■ 수탁자나 개인정보를 제공받은 자가 처리하는 개인정보에 대한 변경 사항이, 개인정보 처리 목적과 관련이 있을 때 이를 통지받는 절차가 있는가?

- (수탁사) 신청인이 개인정보를 위탁처리 하는 경우, 개인정보의 변경 사항이 있고 이것이 개인정보 처리 목적과 관련될 때에는 신청인과 수탁사 간에 대해 이러한 정보 공유가 이루어져야 한다. 신청인 또는 수탁사가 정확하지 않는 정보 등을 확인하는 경우 이를 서로에게 신속히 통지하고 반영하는 절차를 마련해야 한다.

- 만약 수탁사가 신청인의 개인정보처리시스템을 공동으로 이용하거나, 신청인과 수탁사가 개인정보처리시스템의 DB를 연동하여 동기화 하는 경우 개인정보 변경에 효과적으로 대응할 수 있다. 자동화가 어려운 경우, 수탁 업무의 수행 주기, 처리되는 개인정보의 특성 등을 고려하여 주기적으로 변경 사항에 대해 통지할 수도 있다.

- (제3자) 신청인이 개인정보를 제3자에게 제공하는 경우, 제3자가의 개인정보 처리에 대한 신청인의 직접적인 관리·감독 등의 책임은 없으나, 정보주체를 위한 최선의 개인정보 보호 및 처리를 위해 신청인의 자발적 책임성이 요구된다.
  - 특히 신청인의 개인정보 처리와 지속적인 관련이 있는 제3자 제공, 예를 들어 계열사 간 공유, 타사와의 서비스 제휴 등의 경우에 이러한 조치가 요구되며, 제3자와 개인정보 변경 현황에 대해 통지하는 기준과 절차 등을 마련하여 상호간에 처리하는 개인정보의 최신정보를 유지하여야 한다.

증적 자료

- 신청인-수탁사 간 개인정보 파일 제공, 갱신과 관련한 업무 매뉴얼 등
- 수탁사와 연계된 개인정보처리시스템 운영 현황
- 계열사, 제휴사 등의 개인정보 제3자 제공과 관련한 업무 협약서

결함 사례

- 신청인과 수탁사의 개인정보처리시스템(DB)가 연동되어 있으나 동기화가 월1회만 진행되고 있어 수탁사가 실시간 최신화되지 않은 개인정보를 이용하고 있는 경우
- A제휴사와 공동 서비스를 진행 중이나 신청인이 접수한 고객의 개인정보 변동 사항에 대해 상대 제휴사에게 통지하는 절차나 시스템이 없는 경우

개인정보 보호법과 비교

- 개인정보 보호법은 수탁자에 의한 개인정보처리에 대한 개인정보처리자의 책임성, 관리·감독의 의무 등을 명확히 규정하고 있으나, 개인정보를 제3자에게 제공한 경우에는 해당 제3자의 개인정보 처리에 대해 강제적 또는 권고적 책임을 규정하지 않는다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제3조(개인정보 보호 원칙)

관련 ISMS-P 인증기준

- 3.2.2 (개인정보 품질보장) 수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체(이용자)에게 관리절차를 제공하여야 한다.

6. 보호 대책

6. 보호 대책

6.1 보호대책 수립/이행	6.2 보호대책 평가/개선
6.3 수탁사의 보호대책	6.4 제3자의 보호대책
6.5 파기	6.6 임직원 인식제고

6.1 보호대책 수립/이행

6.1.1 보호대책 수립

26. 개인정보 보호를 위한 보호대책을 수립해야 한다.

6.1.2 보호대책 구현

27. 개인정보의 분실, 불법적인 접근, 파기,이용, 수정, 제공 또는 기타 오용의 위험으로부터 보호하기 위한 물리적, 기술적 및 관리적 보호대책을 수립하고 구현해야 한다.

주요 확인사항

- ■ 개인정보 보호를 위해 물리적, 기술적, 관리적 보호대책을 마련하여 시행하고 있는가?
- ■ 개인정보 보호대책 요구사항은 신청인의 개인정보 처리의 특성에 맞게 적절한 항목으로 구성되었는가?

- 신청인은 개인정보 보호를 위해 물리적, 기술적, 관리적 보호대책을 마련하여야 한다. 사내 모든 개인정보 보호에 관한 최상위 수준의 근거 규정인 개인정보 보호 정책이나 지침에 보안정책을 포함하거나 별도의 문서로 마련할 수도 있다.

- 보호대책은 개인정보의 성질이나 처리 환경 등 개인정보 처리의 특성에 따라 요구되는 조치 사항들로 마련되어야 할 것이며, 다음의 항목*들이 포함될 수 있다.

* 국내 개인정보 보호법의 「개인정보의 안전성 확보조치 기준」의 내부관리계획 항목 참고

기술적 보호조치

- 접근 권한 관리 : 업무 수행에 필요한 최소한의 범위로, 차등 부여
- 접근 통제 : 접속 제한 등 불법적인 접근 방지 및 유출 탐지 등 침해사고 방지
- 개인정보의 전송 또는 저장 시 암호화
- 개인정보처리 시스템에 대한 접속기록 보관 및 점검
- 백신 프로그램 설치 등 악성프로그램 방지 및 치료

관리적 보호조치

- 보호대책을 위한 조직 구성 및 운영
- 위험 평가, 취약점 점검 등
- 개인정보 유출사고 시 신고, 대책 마련 등 대응
- 수탁사의 보호대책 요구 및 관리·감독

물리적 보호조치

- 잠금장치, 출입 통제 등 물리적 보호조치

증적 자료

- 개인정보 보호 정책/지침
- 개인정보 보호 내부관리계획 등 보안대책에 관한 내부 정책/지침

결함 사례

- 문서화된 개인정보 보호대책이 없거나 보안대책의 항목이 신청인의 개인정보 처리의 특성을 적절히 반영하지 못한 경우

• 개인정보 보호법과 비교 •

내부관리계획에 포함되어야 하는 사항(개인정보 보호법 시행령 제30조)

개인정보처리자	정보통신서비스 제공자등
1. 개인정보 보호책임자의 지정에 관한 사항 2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 3. 개인정보취급자에 대한 교육에 관한 사항 4. 접근 권한의 관리에 관한 사항 5. 접근 통제에 관한 사항 6. 개인정보의 암호화 조치에 관한 사항 7. 접속기록 보관 및 점검에 관한 사항 8. 악성프로그램 등 방지에 관한 사항 9. 물리적 안전조치에 관한 사항 10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항 11.개인정보 유출사고 대응 계획 수립·시행에 관한 사항 12. 위험도 분석 및 대응방안 마련에 관한 사항 13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항 14. 개인정보 처리업무를 위탁하는 경우 수탁사에 대한 관리 및 감독에 관한 사항 15. 그 밖에 개인정보 보호를 위하여 필요한 사항	1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항 2. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항 3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항 4. 개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항 5. 개인정보 처리업무를 위탁하는 경우 수탁사에 대한 관리 및 감독에 관한 사항 6. 개인정보의 분실·도난·유출·위조·변조·훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항 7. 그 밖에 개인정보 보호를 위해 필요한 사항 8. 개인정보 보호책임자 및 개인정보취급자에 대한 교육에 관한 사항 9. ·개인정보의 기술적·관리적 보호조치 기준 제4조~제8조까지의 보호조치 이행을 위한 세부적인 추진방안 - 제4조 : 접근통제 - 제5조 : 접속기록의 위·변조 방지 - 제6조 : 개인정보의 암호화 - 제7조 : 악성프로그램 방지 - 제8조 : 물리적 접근 방지

- 개인정보 보호법에 따라 개인정보처리자는 개인정보 보호를 위한 내부관리계획을 수립하여 시행하여야 하며, 내부관리계획에는 개인정보 보호책임자 지정, 개인정보 보호 교육 및 기술적 보호조치 사항 등 다음의 사항들이 포함되어야 한다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제29조(안전조치 의무)
- 개인정보 보호법 제39조의5(개인정보의 보호조치에 대한 특례)
- 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
- 개인정보 보호법 시행령 제48조의2(개인정보의 안전성 확보 조치에 관한 특례)
- 개인정보의 안전성 확보조치 기준(고시)
- 개인정보의 기술적 관리적 보호조치 기준(고시)

관련 ISMS-P 인증기준

- 1.2.4(보호대책 선정) 위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
- 1.3.1 (보호대책 구현) 선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행 결과의 정확성과 효과성 여부를 확인하여야 한다.

6.1.3 비례적 보호대책

28. 개인정보의 물리적, 기술적 및 관리적 보호대책은 개인정보 침해 위협의 가능성 및 심각도, 개인정보의 민감성, 그리고 개인정보를 처리하는 특성과 비례하는 수준이여야 한다.

주요 확인사항

- ■ 위험평가 등을 통해 위험을 식별하고 평가하여 그에 따른 비례적인 보호대책을 마련하였는가?
- ■ 위험을 식별하는 기준은 개인정보 침해 위험의 발생 가능성, 심각성 및 개인정보의 민감성 그리고 개인정보의 처리 환경(상황)을 고려하였는가?

- 개인정보의 안전성 확보를 위해서는 모든 가능한 침해 위험에 대해 대비하는 것이 바람직하나 한정된 인력, 비용 등을 포함한 자원으로는 현실적으로 불가능하다. 따라서 이용 가능한 자원 내에서 물리적, 기술적 보호조치의 효과적인 구현하여 최대의 효과를 얻기 위해 위험 발생 가능성이나 발생 시 심각성 등을 식별하는 위험평가의 과정이 필요하다.
- 위험평가의 방법은 다양하게 있으나 일반적으로 다음의 순서를 따른다.
  1) 개인정보와 관련한 정보자산을 식별하고, 중요도를 평가한다.
  2) 정보자산, 서비스에 대한 위협과 취약성, 위험을 식별한다.
  3) 각 정보자산, 서비스에 대하여 해당 위험의 발생가능성, 위험도 등을 평가한다.
  4) 평가한 위험도 중 수용 가능한 위험수준(DoA)을 결정한다.
  5) 수용 가능한 수준을 넘어선 위험에 대한 대비책을 마련하여 이행한다.
- 수용 가능한 위험수준(DoA, Degree of Assurance)이란 모든 위험을 조치하기에는 자원(인력, 시간, 비용)이 부족하기 때문에 신청인이 가능한 수준에서 조치할 위험을 결정, 즉 비례적 보호조치가

필요하다. DoA 이하의 위험의 경우 위험을 수용하기 때문에 DoA의 결정에는 경영진의 승인이 필요하다.

- 위험에 대한 처리는 일반적으로 다음과 같은 방법을 사용하지만 효과성이 검증된 다른 방법도 가능하다.
  - 위험 수용 : 위험으로 인한 피해(손실)을 감수함. 보통 위험의 발생가능성이 낮거나 위험을 제거하기 위한 비용이 많이 드는 경우로 DoA이하의 위험인 경우이다.
  - 위험 제거/감소 : 자원을 투입하여 위험의 발생가능성을 줄이는 방법이다. 보통 DoA이상의 위험에 대하여 조치를 취하여 DoA이하 수준으로 낮춘다.
  - 위험 회피 : 위험 때문에 관련 사업이나 프로세스를 포기한다.
  - 위험 전가 : 보험에 가입하거나 해당 업무를 외주 처리함으로써 제3자에게 위험을 전가한다.
- 일반적으로 위험평가는 보호대책의 적절성을 판단하고 새로운 위험과 위협에 대응하기 위하여 자체 실시 또는 외부 전문기관을 통해 연1회 주기적으로 실시하며, 정보시스템의 대단위 개편, 시스템 도입, 사업의 변경 등 중대한 변화가 있는 경우 비정기적으로 실시할 수 있다.
- 위험평가를 실시할 때에는 전체 사업 또는 정보자산에 대해 실시하거나 인증 범위로만 한정하여 범위를 축소하여 실시하는 것도 가능하다. 위험평가가 어려운 경우 국내 법령에서 요구하는 물리적, 기술적 보안조치를 이행하여야 한다. 특히 개인정보처리자의 경우 보유하고 있는 개인정보의 종류 및 수량에 따라 법령에서 요구하는 보안조치의 내용이 다르다.

증적 자료

- 위험평가와 관련한 내부 개인정보 정책/지침
- 위험평가 계획서, 평가 보고서 및 개선조치 보고서

참고 자료

- 위험평가 관련 자료 (isms.kisa.or.kr의 자료실)

결함 사례

- 신청인이 사업 합병 등을 통해 서비스 확장 후, 정기 위험 평가와 별도로 변경된 시스템과 서비스에 대한 위험 평가를 실시하지 않은 경우

개인정보 보호법과 비교

- 개인정보 보호법의 안전조치 의무 규정에 따라 개인정보처리자는 개인정보 보호를 위한 내부 관리 계획을 수립·시행해야 하며, 본 내부 관리 계획에는 위험도 분석 및 대응방안 마련을 포함하도록 했다. 위험도 분석이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험 요소를 식별, 평가하고 해당 위험 요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합으로 분석하는 행위로 정의하였다. 또한 위험 요소로 고의 과실 등 관리적, 해킹 등 기술적, 비인가자 출입 등 물리적 요소로 설명하였다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제29조(안전조치 의무)
- 개인정보 보호법 제39조의5(개인정보의 보호조치에 대한 특례)
- 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
- 개인정보 보호법 시행령 제48조의2(개인정보의 안전성 확보 조치에 관한 특례)
- 개인정보의 안전성 확보조치 기준(고시)
- 개인정보의 기술적 관리적 보호조치 기준(고시)

관련 ISMS-P 인증기준

- 1.2.3 (위험 평가) 조직의 대내외 환경 분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.

- 1.2.4 (보호대책 선정) 위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.

6.1.4 보호대책 이행

30. 비례성의 원칙에 따라 수립된 보호대책을 효과적으로 구현하고 이행해야 한다.

6.1.5 보호대책 요구사항

32. 내외부 침입, 공격에 의한 개인정보 침해사고를 예방하고 사고 발생 시 체계적으로 대응하기 위한 대책을 수립하고 이행해야 한다.

주요 확인사항

■ 신청인이 수립한 보호대책을 적용하여 개인정보 처리 절차를 마련하고, 개인정보처리 시스템 등을 구현하였는가?

■ 보호대책을 실제 이행하고 이러한 보호대책이 정확하고 효과적인지 확인하였는가?

- 개인정보 보호대책은 개인정보 처리의 특성에 비례하여 수립하여야 하며, 개인정보 처리 절차, 개인정보처리시스템 등은 이러한 보호대책을 반영하여 개발, 구현되어야 한다. 또한 실제 보호대책을 이행하기 위한 이행 계획을 수립하고 보호대책의 목적을 정확하고 효과적으로 달성하는지 여부를 확인해야 한다.

증적 자료

- 보호대책 이행계획서, 이행 완료 보고서

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제29조(안전조치 의무)
- 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
- 개인정보의 안전성 확보조치 기준(고시)
- 개인정보의 기술적 관리적 보호조치 기준(고시)

관련 ISMS-P 인증기준

- 1.3.1 (보호대책 구현) 선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.
- 2.11.1(사고 예방 및 대응체계 구축) 침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.

6.2 보호대책 평가/개선

6.2.1 보호대책 평가

> **33. 개인정보 보호대책의 이행 여부, 효과성 등을 평가하기 위한 절차와 방법을 마련하고 정기적으로 실시해야 한다.**

6.2.2 보호대책 개선

> **34. 개인정보 보호대책에 대한 평가 결과 확인된 문제점에 대해 개선책을 마련하고 보호대책에 반영해야 한다.**

주요 확인사항

- ■ 개인정보 보호대책의 적절한 이행, 효과성 검증을 위한 주기적인 평가를 실시하는가?
- ■ 평가 결과 발견된 개선 사항에 대해 개인정보 보호 정책에 반영하는가?

- 개인정보 보호대책이 적절히 이행되고, 효과적으로 작용하는지 여부에 대해 정기적으로 점검해야 한다. 점검주기, 점검 기준 및 방법, 수행 인력 등에 대한 점검 계획을 수립하고 이행한다. 내부 전문 인력을 통한 자체 점검 또는 외부 개인정보 보호 관련 인증 또는 평가 수행기관을 통한 점검도 가능하다. 점검 범위는 내부 정책뿐만 아니라 관련 법령, 보안 기술 등 내외부 환경 변화를 적절히 반영하는지 여부도 포함한다.
- 평가 결과 확인된 취약점 등 문제점에 대해서는 개선책을 마련하여 보호대책에 반영해야 한다.

증적 자료

- 보안대책 점검 계획서 및 결과보고서
- 보안대책 개선 계획서 및 개선조치 결과서

• 관련 법령 •

관련 개인정보 보호법 법조항 및 지침 등

• 해당 사항 없음

• 관련 ISMS-P 인증기준 •

- 1.4.2(관리체계 점검) 관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
- 1.4.3(관리체계 개선) 법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.

6.3 수탁사의 보호대책

6.3.1 수탁사 보호 체계

46. 수탁사가 신청인의 개인정보 보호 정책을 이행하도록 하기 위해 문서화된 체계를 마련해야 한다.

6.3.2 수탁사 보호대책

35. 위탁 처리하는 개인정보의 분실, 불법적인 접근, 파기, 이용, 수정, 제공 또는 기타 오용의 위험으로부터 보호하기 위해 수탁사에게 보호대책 이행을 요구해야 한다.

6.3.3 수탁사 보호조치 요구 사항

47. 수탁사의 개인정보 보호 조치를 위한 요구 사항에는 다음의 사항이 포함되어야 한다.

- 신청인의 개인정보 보호 정책 및 업무 관행 준수 또는 이와 실질적으로 유사한 수준의 업무 관행 수행
- 신청인의 개인정보 처리 방식과 관련하여 신청인의 지시 사항 준수
- 신청인의 동의 없는 재위탁 제한
- 개인정보 침해 발생 시 신청인에게 통지 요구

주요 확인사항

■ 수탁사와 계약 체결 시 수탁사의 개인정보 보호 조치 수준을 확인하기 위한 기준이나 절차가 있는가?

■ 수탁사가 신청인의 개인정보 보호 수준을 이행할 수 있도록 수탁사에게 적용되는 다음의 개인정보 보호 체계를 확인 또는 마련하는가?

- 개인정보 보호 관련 수탁사의 내부 지침 또는 정책 확인
- 개인정보 처리와 관련한 계약 체결
- 관할 개인정보 보호 관련 법령 준수 요구
- 관할 개인정보 보호 관련 자율규제 프로그램/행동규약 준수 요구

■ 수탁사가 귀사의 개인정보 보호 정책을 충족하도록 하기 위해 다음을 포함한 조치를 요구하는가? 다음 항목 외 추가적인 사항은 무엇이 있는가?

- 신청인의 개인정보 보호 정책 및 업무 관행 준수 또는 이와 실질적으로 유사한 수준의 업무 관행 수행
- 신청인의 개인정보 처리 방식과 관련하여 신청인의 지시 사항 준수
- 신청인의 동의 없는 재위탁 제한
- 개인정보 유출 사고 발생 시 신청인에게 통지 요구
- 보안침해 사고 발생 시 신속한 대처 및 신청인에게 통지 요구

- 개인정보 처리 업무를 위탁은 개인정보 처리를 실질적으로 제3자가 수행하지만, 신청인 본인인의 업무 처리와 이익을 위한 것이며, 처리하는 개인정보에 대한 관리·지배권이 신청인에 있는 경우를 말한다. 지배권이 제3자에게 이관되는 제3자 제공과 구분된다.

- 따라서 개인정보 처리 주체는 여전히 신청인이며 수탁사의 개인정보 처리에 대한 교육, 관리·감독 책임 등이 있다. 이에 신청인은 개인정보 보호와 관련하여 신청인에 적용되는 법적 의무사항을 수탁사가 준수하도록 해야 한다. 이를 위해 다음의 방법으로 수탁사의 보호 조치 수준을 확인하거나 이행 방안을 마련할 수 있다.
  - 신청인의 내부 개인정보 보호 정책/지침에 반영
  - 수탁사와 체결하는 계약서에 해당 내용 포함

- 수탁사의 개인정보 보호 관련 법령 준수 여부 확인
- 수탁사의 개인정보호호 관련 자율규제 규약/규칙 준수 여부 확인

- 이에 더해, 신청인은 수탁기관이 준수하고 있는 규범/지침 등이 신청인의 CBPR 원칙에 따른 개인정보 보호 원칙을 충족하는지 반드시 확인하고, 계약서를 통해 이를 포함한 요구 사항을 반영해야 한다. 계약서에는 이 외에도 업무 위탁의 범위와 양 당사자 간의 책임 관계가 명확히 기술되어야 한다.

- 계약서에는 수탁사의 위탁 업무 범위 외 개인정보 이용·제공 금지, 개인정보 보호를 위한 보안조치, 재위탁 제한 등 구체적인 사항을 포함하여야 한다. 적절하다고 판단하는 경우 수탁사에게 CBPR과 같은 개인정보 보호 인증 취득을 요구할 수도 있다. 국내 개인정보 보호법에서는 수탁사와의 계약서에 포함되어야할 사항을 다음과 같이 규정하고 있어 이를 참고하여 마련할 수 있다. 이외에도 위탁자가 필요하다고 판단되는 개인정보에 관한 사항을 추가로 문서(부속합의서 등)에 반영할 수 있다.

(개인정보 보호법) 위수탁 계약에 포함되어야 하는 항목

① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
② 개인정보의 기술적·관리적 보호조치에 관한 사항
③ 위탁업무의 목적 및 범위
④ 재위탁 제한에 관한 사항
⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
⑥ 위탁업무와 관련하여 교육, 개인정보의 관리 현황 점검 등 감독에 관한 사항
⑦ 수탁사가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

- 또한 이러한 개인정보 보호 원칙이 지속적으로 잘 이행되고 있는지 확인하기 위해 수탁사 점검 계획을 마련하고 주기적으로 점검한다. 점검 등 관리·감독에 대한 사항은 【CBPR 자가 평가 질문 48~49】를 참고한다.

증적 자료

- 적용 대상 개인정보 보호 관련 법령 목록
- 개인정보처리 업무 위수탁 계약서, 개인정보 보호 협약서(약정서, 부속합의서)
- 개인정보 처리 업무 위탁관련 내부 지침

결함 사례

- 개인정보 처리업무 일부를 외부업체에 위탁하고 있으나 문서화된 계약서 없이 단편적인 업무 지시에 따라서 업무를 수행하는 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 개인정보처리자가 업무 위탁 시 개인정보의 안전한 관리를 위한 위탁사 및 수탁사의 최소한의 조치 사항을 규정하였다. 그리고 이와 함께 위탁하는 업무의 범위 등을 문서로 작성하도록 명시하였다.

- 특히 수탁사에 대한 안전성 확보조치 교육 및 관리·감독, 수탁사의 위법한 개인정보 처리에 대한 손해배상 책임 등 개인정보처리자의 책임성에 대해 명확히 규정하였다. 그러나 동시에 수탁사도 이 법의 개인정보 처리에 관한 주요 의무를 준용하도록 규정하여 수탁사에 대한 처벌도 가능하도록 했다.

※「개인정보 처리 위수탁 안내서」를 통해 위탁사 및 수탁사의 단계별 조치 사항을 구체적으로 안내

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
- 개인정보 보호법 시행령 제28조(개인정보의 처리 업무 위탁 시 조치)
- 개인정보 처리 위수탁 안내서('20.12월)

• 관련 ISMS-P 인증기준 •

- 2.3.1 (외부자 현황 관리) 업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생되는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.

- 2.3.2 (외부자 계약 시 보안) 외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보 보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.

- 2.3.3(외부자 보안 이행 관리) 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보 보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.

6.3.4 수탁사 관리·감독(자체평가)

48. 수탁사의 개인정보 보호 조치 이행 여부를 주기적으로 점검할 수 있는 체계를 마련해야 한다.

– (예) 수탁사에게 주기적 자체평가 실시 및 결과 제출 요구

6.3.5 수탁사의 관리·감독(현장점검)

49. 수탁사의 개인정보 보호 조치 이행 여부를 주기적으로 점검할 수 있는 체계를 마련해야 한다.

- (예) 수탁사 대상 정기적 현장 점검 또는 모니터링 수행

주요 확인사항

■ 수탁사가 개인정보 처리에 대한 계약/합의 등을 이행하고 있는지 여부를 주기적으로 점검하는가?

■ 각 수탁사 별 점검하는 방법과 점검 항목은 무엇이며 이는 수탁하는 개인정보 처리의 특성에 적절한가?
-예 : 수탁사에게 자체 평가 보고서 작성 및 제출 요구, 수탁사에 대한 정기적 모니터링이나 현장 점검 등

■ 수탁사에 대한 점검 또는 감사 시 발견된 문제점에 대하여 수탁사가 개선계획을 수립 및 이행하고 그 결과를 제공하고 있는가?

- 신청인은 계약서 등을 통해 합의된 개인정보 보호 조치를 이행하고 있는지 여부에 대해 관리·감독할 책임이 있다. 따라서 신청인은 수탁사와 협의하여 수탁자에 대한 점검 계획을 수립하고 정기적으로 이를 이행해야 한다.

- 수탁사 점검은 신청인이 내부 개인정보 보호 정책과 위수탁 계약서를 바탕으로 위탁 기간, 수탁사의 개인정보 보호 역량, 위탁하는 개인정보 업무의 성격, 그리고 처리하는 개인정보의 민감도 등을 고려하여 점검 항목과 방법, 점검 주기 등을 정한다.

- 신청인은 원격 모니터링 및 현장 방문하여 점검하는 등 직접 수행하거나 수탁사에게 자체 점검하여 결과를 제출하도록 요구할 수 있다. 또는 이러한 직접적인 관리·감독이 현실적으로 어려운 상황이 있는 경우에는, 수탁사의 개인정보관리 이행 수준을 판단할 수 있는 대체 방안(정부 등 외부 감독 체계, 인증 등)을 활용 수 도 있다.

- 수탁사 점검은 업무 시작 전, 계약이 유지되는 과정, 종료 시점 모두 적용되며, 이 중 위수탁 계약이 종료되거나 담당자 변경 등의 경우 정보자산 반납, 정보시스템 접근계정 삭제, 개인정보 파일 파기 또는 반납 여부 등을 확인하여야 한다.

- 신청인은 점검 및 감사 결과에 대하여 공유하고 발견된 문제점에 대한 개선방법 및 재발 방지대책을 수립하여 이행하도록 확인하여야 한다.
  - 개선조치 완료 여부 확인을 별도의 이행점검을 직·간접적으로 수행하여야 한다.

증적 자료

- 수탁사 보안점검 계획서 및 점검 체크리스트
- 수탁사 보안점검 및 결과보고서, 개선조치 결과보고서

결함 사례

- 개인정보 처리 시스템 개발 및 운영 업무를 수행하는 외주업체에 대해서 정기적으로 보안점검 및 감사를 수행하고 있지 않은 경우
- 수탁사가 자체적으로 보안점검을 수행한 후 그 결과를 통지하도록 하고 있으나, 수탁사가 보안점검을 충실히 수행하고 있는지 여부에 대하여 확인하는 절차가 존재하지 않아 보안점검 결과의 신뢰성이 떨어지는 경우

개인정보 보호법과 비교

- 개인정보 보호법은 개인정보 처리 업무 위탁 시 위수탁 계약서, 협약서 등 문서를 통해 위탁하는 업무의 범위, 개인정보의 안전한 관리를 위한 위탁사 및 수탁사 상호간의 책임과 의무를 명시하도록 규정했다. 그리고 위탁사는 이 법에 따라 수탁사가 이를 잘 이행하고 있는지 점검하고 관리·감독하여야 한다. 이러한 점검 및 관리·감독에 관한 사항 또한 수탁사와의 협의를 통해 구체적으로 정하고 계약서 등에 반영하도록 명시하였다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
- 개인정보 보호법 시행령 제28조(개인정보의 처리 업무 위탁 시 조치)
- 개인정보 처리 위수탁 안내서('20.12월)

관련 ISMS-P 인증기준

- 2.3.3 (외부자 보안 이행 관리) 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보 보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.
- 2.3.4 (외부자 계약 변경 및 만료 시 보안) 외부자 계약만료, 업무종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 중 취득정보의 비밀유지 확약서 징구 등의 보호대책을 이행하여야 한다.

6.4 제3자의 보호대책

6.4.1 제3자의 보호조치

50. 개인정보를 제3자에게 제공하나 해당 제3자를 대상으로 CBPR 보호 원칙을 준수를 확인하기 위한 실사(due diligence)나 합리적인 조치가 어려운 경우에도, 제공된 개인정보에 대한 최소한의 보호 수준을 확인하기 위한 조치를 강구해야 한다.

주요 확인사항

- ■ 개인정보를 제3자에게 제공하는 경우, 제공 이전에 해당 제3자의 개인정보 보호 수준을 확인하는가?
- ■ APEC CBPR의 개인정보 보호 원칙을 준수하지 않는 제3자 또는 보호 수준 확인이 어려운 제3자에게 개인정보를 제공하는 경우 제공되는 개인정보의 최소한의 보호를 위한 다른 방법을 마련하는가?
- ■ 개인정보 제3자 제공에 대해 정보주체의 동의를 받는 경우, 동의 내용에 대해 명확히 알리고 동의 의사를 확인하는 방법으로 동의를 받는가?

- 개인정보를 제3자에게 제공하는 경우, 제공받는 자가 새로운 개인정보처리자로써 제공받은 개인정보 처리에 대한 책임을 진다. 따라서 신청인은 제공된 개인정보에 대한 직접적인 관리·감독의 의무가 없다. 그러나 CBPR 원칙에서는 정보주체의 개인정보 보호에 대한 최소한의 보장을 위해 가능한 범위 내 책임 있는 조치를 취할 것을 요구한다.

- 이에 신청인은 개인정보를 제3자에게 제공하기 전 해당 제3자가 CBPR 개인정보 보호 원칙을 준수하는지 여부를 확인하고 가급적 개인정보 보호 수준을 갖춘 자에게 제공한다. 제3의 보호 수준 확인이 어렵거나 CBPR 보호 원칙을 이행하지 않는 제3자의 경에 제공하는 경우, 그 이유를 확인하고 이를 보완 또는 대체할 수 있는 다른 방법을 마련하여 개인정보가 보호될 수 있도록 조치해야 한다. 제3자의 개인정보 보호 수준 확인을 위해 개인정보 보호·정보보호 인증마크 획득, 자율규약 프로그램 참여 여부 및 내부 정책 수립 여부 등을 살펴볼 수 있다.

- 또한 개인정보 제공 과정에서 개인정보 유출, 분실, 훼손 등 침해 사고가 발생하지 않도록 개인정보 파일 및 전송 시 암호화, 접근 권한 관리 등 안전성 확보 조치를 해야 한다.

- 개인정보 제3자 제공에 대한 정보주체의 동의를 받는 경우에는 정보주체의 자유로운 의사 결정에 의한 명시적 동의가 되도록 절차를 마련하고 이를 입증할 수 있어야 한다. 즉 동의를 받을 때에는

제공받는 자, 제공목적, 제공항목 등 동의하는 사항에 대한 정보를 충분히 제공하고 동의 여부 의사를 명확히 확인할 수 있도록 절차를 마련해야 한다. 국내 개인정보 보호법에서는 개인정보 제공에 대한 동의 시 다음의 사항을 알리고 동의 받도록 규정하고 있어 이를 참고할 수 있다.

(개인정보 보호법) 개인정보 제3자 제공 시 고지 사항

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

증적 자료

- 개인정보 제공에 관한 절차 및 제공 내역
- 개인정보 제공 동의 절차 및 동의서 샘플
- 개인정보 제공에 대한 계약서(합의서)

결함 사례

- 개인정보 제공에 대한 정보주체의 동의 획득 시 제공 목적, 제공항목 등 동의에 대한 충분한 정보를 제공하지 않거나 동의 칸에 미리 표시(예: (☒)를 해놓은 경우

• 개인정보 보호법과 비교 •

- 개인정보 보호법은 개인정보 제3자 제공 시 정보주체로부터 명시적 동의 등 적법한 절차로 동의를 받아야 할 것을 규정하고 있고, 제공된 개인정보에 대한 추가적인 보호 의무는 부과하지 않는다. 이외 개인정보를 제공받는 자에 대해서는 정보주체의 동의나 법률의 특별한 규정이 있는 경우를 제외하고, 제공받은 목적 외의 용도로 이용하거나 다른 제3자에게 제공하는 것을 제한하고 있다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)
- 개인정보 보호법 제19조(개인정보를 제공받은 자의 이용·제공 제한)

• 관련 ISMS-P 인증기준 •

- 3.3.1(개인정보 제3자 제공) 개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체(이용자)의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.

6.5 파기

6.5.1 파기

31. 개인정보의 안전한 파기 정책을 마련하고 이행해야 한다.

주요 확인사항

- ■ 개인정보 파기에 관한 정책이 마련되어 있는가?
- ■ 개인정보의 처리 목적이 달성된 경우 지체 없이 파기하고 있는가?
- ■ 파기 정책에 따라 안전하게 개인정보를 파기하고 있는가?

- 개인정보의 처리 목적이 달성되었거나 보유기간 경과 시에는 그 개인정보를 지체 없이 파기하여야 한다. 개인정보를 안전하기 파기하기 위한 내부 정책을 마련하고, 정책에는 파기책임자 및 담당자의 지정, 수집 목적별 개인정보의 보유기간파기 방법, 파기 절차, 파기 기록의 작성과 관리 등의 사항을 포함한다.

- 개인정보를 파기할 때에는 복구 및 재생이 불가능한 방법을 사용하여야 한다.
  - 문서의 경우 파쇄, 소각 등
  - 전자적 저장 매체의 경우 데이터를 영구 삭제(디가우징 기술 등 사용)하고, 저장 매체를 재사용해야 하는 경우 복구가 불가능한 방법으로 삭제(덮어쓰기 등)
  - DBMS(데이터베이스 관리시스템)와 같이 계속 유지해야 하는 설비의 경우 해당 셀의 내용을 무의미한 값으로 변경 등

증적 자료

- 개인정보 파기에 관련한 내부 개인정보 정책/지침
- 개인정보 파기 기록

결함 사례

- 개인정보가 담긴 이동형 저장매체를 1회 포맷하고 재사용하고 있어 기존의 정보가 복구가 가능한 경우
- 탈퇴한 회원의 이름과 연락처 정보 등 일부 정보만 삭제하고, ID, 이용 내역 등은 보유하는 경우

개인정보 보호법과 비교

- 개인정보 보호법은 개인정보 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때는 지체 없이 파기하도록 했고, 파기 시에는 복원이 불가능한 방법으로 영구 삭제 또는 파쇄·소각 등의 방법으로 하도록 규정했다. 또한 다른 법령에 따라 개인정보를 파기하지 않고 보존해야하는 경우에도 해당 개인정보를 다른 개인정보와 분리하여 저장·관리하도록 했다. 정보통신서비스 제공자의 경우에는 이외에도 1년 이상 서비스를 이용하지 않는 이용자의 개인정보에 대해서는 파기 또는 다른 이용자의 개인정보와 분리 보관하도록 했다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제21조(개인정보의 파기)
- 개인정보 보호법 제39조의6(개인정보 파기에 관한 특례)

관련 ISMS-P 인증기준

- 3.4.1 (개인정보의 파기) 개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.

6.6 임직원 인식제고

6.6.1 임직원 인식제고

> **29. 임직원을 대상으로 교육훈련 등 개인정보 보호의 중요성에 대한 인식제고를 위한 활동을 실시해야 한다.**

6.6.2 임직원 교육

> **44. 개인정보 민원 대응을 포함하여 개인정보 보호 정책 및 절차에 대한 직원 교육 절차를 수립하여야 한다.**

주요 확인사항

- ■ 교육 내용, 대상, 주기 및 방법, 교육 효과에 대한 평가 등 교육 운영에 대한 사항을 정하여 문서화하였는가?
- ■ 개인정보 보호 교육 내용은 관련 법령, 위반 시 법적 책임, 사내 정책 등을 포함하고 있는가?
- ■ 개인정보 관련 민원 처리에 대한 교육을 하는가? 민원처리 매뉴얼 또는 교육 자료가 마련되었는가?
- ■ 개인정보 보호 교육은 정기적으로 실시하고 있는가?

- 개인정보를 취급하는 내부 임직원 또는 외부 수탁사 등 개인정보취급자에 대한 개인정보 보호 인식을 제고하기 위한 조치를 이행하여야 한다. 이를 위해 개인정보취급자에 대한 교육 계획을 수립하여 정기적으로 개인정보 보호에 관한 교육을 시행하고 그 기록을 보관하여야 한다.
- 교육 내용은 개인정보 보호 관련 법령, 침해사고 사례, 규정 위반 시 법적 책임, 보호대책 등을 비롯하여 사내 개인정보 보호 정책 및 민원 처리 등 업무별 개인정보취급자의 조치 사항을 포함한다.
- 교육 방법은 개인정보처리자의 직무, 교육 여건 등을 고려하여 온라인, 오프라인 교육 또는 내부 인력 활용, 외부 전문가 또는 교육 전문기관에 위탁, 또는 전체 교육, 그룹 세미나 등 효과적인 방법을 선택하여 진행할 수 있다. 이외에도 관련 임직원 대상 개인정보 보호 서약서를 징구하고 정기적으로 재징구할 수 있다. 퇴직 또는 계약 만료 시에도 비밀유지서약서를 징구한다.
- 신규 인력, 외부 인력 등이 개인정보 업무를 수행하기 전에 교육을 수행하여야 하며, 특히 개인정보를 외부에 처리 위탁한 경우 수탁업체를 대상으로 직접 또는 교육 수행 여부를 확인하여야 한다.

- 교육 종료 후에는 설문조사, 시험 등을 통해 교육 효과를 분석하여 다음 교육에 반영할 수 있도록 한다. 이 외에도 개인정보 보호의 중요성을 인지시키기 위해 캠페인 실시, 수칙 개발 등 다양한 인식제고 활동을 정기적으로 수행할 수 있다.

증적 자료

- 개인정보 교육 및 인식제고에 관련한 내부 개인정보 정책/지침
- 개인정보 교육 계획서 및 결과보고서
- 개인정보 보호 교육자료(영상, 인쇄물 등)
- 사내 및 수탁사 임직원 보안서약서 샘플

결함 사례

- 개인정보 보호 교육을 정기적으로 실시하나 교육 이수자 관리를 하지 않아 미수자에 대한 교육(온라인 교육, 전달교육 등)이 없는 경우
- 개인정보 민원처리 교육 대상에 외주 고객센터 직원이 누락되어 개인정보 민원 교육을 받지 않은 경우

개인정보 보호법과 비교

- 개인정보 보호법은 개인정보의 안전한 관리를 위해 개인정보를 취급하는 임직원을 비롯하여 파견근로자, 시간제근로자 등에 정기적으로 필요한 교육을 실시하도록 규정하였다. 또한 내부 관리계획을 수립하여 개인정보 보호 교육 실시에 관한 사항을 명시하도록 하였다.

관련 개인정보 보호법 법조항 및 지침 등

- 개인정보 보호법 제28조(개인정보취급자에 대한 감독)
- 개인정보의 안전성 확보조치 기준 및 해설서('20.12)
- 개인정보의 기술적·관리적 보호조치 기준 및 해설서('20.12)

관련 ISMS-P 인증기준

- 2.2.3 (보안서약) 정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법령, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.

- 2.2.4 (인식제고 및 교육훈련) 임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.

APEC CBPR 안내서

APEC Cross Border Privacy Rules



개인정보보호위원회
Personal Information Protection Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY