

발 간 등 록 번 호

11-1790365-100007-01

개인정보 손해배상책임 보장제도 안내서

2024. 3.



개인정보보호위원회

Personal Information Protection Commission

발 간 등 록 번 호

11-1790365-100007-01

개인정보 손해배상책임 보장제도 안내서

2024. 3.



개인정보보호위원회

Personal Information Protection Commission

개인정보 손해배상책임 보장제도 안내서

안내 사항

발간 목적

본 안내서는 「개인정보 보호법」에 따라 개인정보 손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준 등에 관한 사항을 안내합니다.

제·개정 이력

개인정보보호 관련 법·제도 및 환경 변화를 반영하여 다음과 같이 개정하였습니다.

일자	주요 내용
'19. 6. 발간	'개인정보 손해배상책임 보장제도' 시행에 따라 관련 내용 안내
'20.12. 개정	「개인정보 보호법」 개정('20년) 사항 반영 및 소관 부처 변경(방통위→개인정보위)
'24. 3. 개정	「개인정보 보호법」 개정('24.3.15. 시행) 사항 반영

재검토 기한

안내서의 최신성을 유지하기 위해 발간일(2024년 3월)을 기준으로 매 3년이 되는 시점(매 3년째의 12.31.까지를 말함)마다 보완 및 개선 등의 조치를 취할 예정입니다.

저작권 표시

본 안내서 내용의 무단전재를 금하며, 가공·인용할 때는 출처를 밝혀 주시기 바랍니다.

* 출처 : 개인정보보호위원회 「개인정보 손해배상책임 보장제도 안내서」 2024. 3.

문의처

본 안내서 내용 관련 문의는 개인정보보호위원회 분쟁조정과(☎02-2100-3142)로 문의주시기 바랍니다.

관계법령

「개인정보 보호법」 제39조의7 및 같은 법 시행령 제48조의7

※ 법령 최신 자료는 국가법령정보센터(www.law.go.kr), 개인정보 보호 안내서 최신 자료는 개인정보보호위원회 누리집*, 개인정보 포털**을 참고

* 개인정보보호위원회 누리집(www.pipc.go.kr) : 법령 > 법령정보 > 안내서

** 개인정보 포털(www.privacy.go.kr) : 자료 > 자료보기 > 안내서

C O N T E N T S

I	추진배경	1
II	손해배상책임 보장제도 주요내용	1
	1. 적용 대상	1
	2. 보험 최저가입금액(준비금 최소적립금액) 기준	5
	3. 다른 법률에 따른 의무보험 등과의 관계	6
	4. 시정조치 명령 및 과태료	7
	5. 시행일	7
III	관련 규정	8
IV	FAQ (자주묻는 질의답변)	10
V	손해배상책임 보장 의무 적용대상 범위	19
VI	손해보험회사 연락처	20

I

추진 배경

- 「개인정보 보호법」에서는 민간·공공 분야 개인정보처리자의 손해배상책임 이행을 보장하도록 보험 또는 공제(이하 '보험 등'이라 함)에 가입하거나 준비금을 적립하도록 의무화
- 「개인정보 보호법 시행령」에서는 법에서 위임한 의무대상 사업자의 범위, 가입금액 기준 등 마련

< 개인정보 손해배상책임 보장제도 도입 경과 >

- 「정보통신망법」을 개정하여 손해배상책임 보장제도 최초 도입 ('19.6.13. 시행)
- 데이터 3법*을 개정하여 「개인정보 보호법」에 반영 ('20.8.5. 시행)
* 개인정보 보호법, 신용정보법, 정보통신망법
- 「개인정보 보호법」을 개정하여 적용대상을 개인정보처리자 일반으로 확대('24.3.15. 시행)
- 「개인정보 보호법 시행령」을 개정하여 의무대상 조정 및 면제기준 상세화('24.3.15. 시행)

II

손해배상책임 보장제도 주요내용

1

적용 대상

다음 각 호의 요건을 모두 갖춘 개인정보처리자

1. 직전 사업연도의 매출액이 **10억원 이상**일 것
2. 전년도 말 기준 직전 3개월간 그 개인정보가 **저장·관리되고 있는 정보주체 수가 일일평균 1만명 이상**일 것

(「개인정보 보호법 시행령」 제48조의7 제1항)

① 개인정보처리자

- 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 법인, 기관, 단체, 개인 등

⇒ 업종, 영리목적 여부 등에 관계없이 업무를 목적으로 개인정보를 저장·관리하는 개인정보처리자가 대상

② 전년도(법인의 경우 전 사업연도) 매출액이 10억원 이상

- 보험 등에 가입하거나 준비금을 적립해야 할 연도의 전년도(법인의 경우 직전 사업연도)의 매출액이 10억원 이상이어야 함
- 매출액은 법 제39조의7 제1항에 따라 보험 등에 가입하거나 준비금을 적립해야 할 연도의 전년도(전 사업연도) 매출액을 말함
 - 매출액의 범위는 개인정보처리자(법인, 기관, 단체, 개인)의 총 매출액을 의미하며, 직전 사업연도 매출액은 손익계산서상 매출액을 기준으로 함
 - * 다만, 전년도 재무제표가 확정되지 않은 경우, 부가가치세과세표준증명서 상 수입 금액 또는 세무조정계산서의 손익계산서 상 매출액을 기준으로 하는 것도 가능
 - 매출액을 산출하지 않는 기관에서는 「법인세법」 제4조 제3항 제1호에 따른 수익사업에서 생기는 소득을 매출액으로 봄

① 보호위원회는 법 제30조의2 제1항에 따라 개인정보 처리방침을 평가하는 경우 다음 각 호의 사항을 종합적으로 고려하여 평가 대상을 선정한다.

1. 개인정보처리자의 유형 및 매출액(매출액을 산정하지 않는 경우에는 「법인세법」 제4조 제3항 제1호에 따른 수익사업에서 생기는 소득을 말하며, 이하 제32조 및 제48조의7에서 "매출액등"이라 한다) 규모

(「개인정보 보호법」 제31조의2)

① 내국법인에 법인세가 과세되는 소득은 다음 각 호의 소득으로 한다. 다만, 비영리 내국법인의 경우에는 제1호와 제3호의 소득으로 한정한다.

1. 각 사업연도의 소득

③ 제1항 제1호를 적용할 때 비영리내국법인의 각 사업연도의 소득은 다음 각 호의 사업 또는 수입(이하 "수익사업"이라 한다)에서 생기는 소득으로 한정한다.

1. 제조업, 건설업, 도매 및 소매업 등 「통계법」 제22조에 따라 통계청장이 작성·고시 하는 한국표준산업분류에 따른 사업으로서 대통령령으로 정하는 것

(「법인세법」 제4조)

③ 개인정보가 저장·관리되고 있는 정보주체 수가 일일평균 1만명 이상

○ 보험 등에 가입하거나 준비금을 적립해야 할 연도의 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 정보주체 수가 일일 평균 1만명 이상인 경우

○ 개인정보가 저장·관리되고 있는 정보주체 수

- '정보주체 수'는 개인정보처리자가 개인정보를 '저장·보관'하는 정보주체 수를 기준으로 산정

* 일일방문자수, 페이지뷰(PV:page view), 순방문자수(UV:unique visitor) 등과는 무관함

○ 일일평균 1만명 이상

- 정보주체 수 일일평균 = 10월, 11월, 12월 일일 정보주체 수의 총합 ÷ 92(일)

◆ (온오프라인 사업 병행 시 정보 주체 수) 오프라인 사업(매장)과 온라인 서비스를 운영하는 경우의 '정보주체 수' 산정은 개인정보를 수집한 경로가 온·오프라인 여부와는 무관하며, 사업자가 저장하고 있는 정보 주체 수 전부가 포함

◆ (회원·비회원·탈퇴회원·휴면회원) '정보주체 수'와 '회원 수'는 일치하는 개념은 아니며, 회원·비회원·탈퇴회원·휴면회원 여부와는 관계없이 개인정보처리자가 업무처리를 목적으로 저장·관리하고 있는 개인정보에 해당한다면 '정보주체 수'에 포함됨

◆ (임직원) 임직원의 경우 '정보주체 수' 산정 대상에서 제외됨. 다만, 임직원이 개인 정보처리자가 제공하는 서비스를 이용하는 고객일 경우, 고객정보에 포함된 임직원 정보는 산정 대상에 포함

4 면제 대상

○ (공공기관) 의무적용을 면제하되, 아래의 경우 예외적으로 의무 적용

1. 연간 매출액 등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자
(제2조 제5호에 따른 각급 학교 및 「의료법」 제3조에 따른 의료기관은 제외한다)
가. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자
나. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자
2. 직전 연도 12월 31일 기준으로 재학생 수(대학원 재학생 수를 포함한다)가 2만명 이상인 「고등교육법」 제2조에 따른 학교
3. 「의료법」 제3조의4에 따른 상급종합병원
4. 공공시스템운영기관

(「개인정보 보호법」 시행령 제32조 제4항)

○ (비영리법인 및 단체) 비영리법인 혹은 단체가 「개인정보 보호법 시행령」 제48조의7 제1항의 요건을 충족하는 개인정보처리자일 경우 의무 대상이나 아래의 경우 예외적으로 의무 면제

1. 「공익법인의 설립·운영에 관한 법률」에 따라 설립 허가된 공익법인
2. 「비영리민간단체 지원법」에 따라 등록한 단체

(「개인정보 보호법 시행령」 제47조 제2항)

○ (소상공인) 「소상공인기본법」 제2조 제1항에 따른 소상공인으로 아래의 요건을 갖춘 자에게 개인정보 저장·관리업무를 위탁한 경우 의무 면제

1. 「소상공인기본법」 제2조 제1항에 따른 소상공인으로부터 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리 업무를 위탁받은 자
2. 1호에 따라 위탁받은 업무에 대하여 「개인정보보호법」 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 한 자

(「개인정보 보호법 시행령」 제48조의7 제3항)

2

보험 최저가입금액(준비금 최소적립금액) 기준

보험 등에 가입하거나 준비금을 적립할 때 최저가입금액(준비금의 경우 최소적립금액)은 정보 주체 수와 매출액 규모 구간별로 차등 설정
: 최저 5천만원 ~ 최고 10억원

(「개인정보 보호법 시행령」 제48조의7 제4항, 별표 1의4)

1 보험 등 최저가입금액 (준비금 최소적립금액)

- 적용 대상 사업자가 보험 등에 가입하거나 준비금을 적립할 때
최저가입금액(최소적립금액) 기준 : 별표 1의4
- 보험 등 가입과 준비금 적립을 병행하는 경우
 - 보험 등 가입금액과 준비금 적립금액을 합산한 금액이 별표 1의4
에서 정한 최저가입금액(최소적립금액) 이상이어야 함

< 손해배상책임의 이행을 위한 최저가입금액(최소적립금액)의 기준(시행령 별표 1의4) >

가입 대상 개인정보처리자의 가입금액 산정 요소		최저가입금액 (최소적립금액)
매출액	정보주체 수	
800억원 초과	100만명 이상	10억원
50억원 초과 800억원 이하		5억원
10억원 이상 50억원 이하		2억원
800억원 초과	10만명 이상 100만명 미만	5억원
50억원 초과 800억원 이하		2억원
10억원 이상 50억원 이하		1억원
800억원 초과	1만명 이상 10만명 미만	2억원
50억원 초과 800억원 이하		1억원
10억원 이상 50억원 이하		5천만원

- ◆ 매출액 : 전년도(법인의 경우 전 사업연도)의 매출액
- ◆ 정보주체 수 : 보험 등에 가입하거나 준비금을 적립해야 할 연도의 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 일일 정보주체 수 평균
- ◆ 보험가입금액 : 계약상 보상 최고한도액으로, 보험계약자가 보험계약을 체결 시 약정한 금액
- ◆ 보험료 : 보험계약에 의하여 보험계약자가 보험회사에 납입한 금액

② 준비금 적립 방법

- 임의적립금(자본계정)으로 적립하고 주주총회 결의 등을 통해 해당 임의적립금이 「개인정보 보호법」 제39조의7의 의무 이행을 위한 것임을 명확히 하여야 함

- ◆ 준비금 : 회사가 순자산액으로부터 자본액을 공제한 금액(잉여금) 중 일부를 장래 생길지도 모르는 필요에 대비하기 위하여 회사에 적립해 두는 금액
- ◆ 임의적립금 : 법률이 아닌 정관/주주총회의 결의에 의하여 이익을 유보한 것으로, 그 이용 목적과 방법은 회사에서 자유롭게 정할 수 있음

3 다른 법률에 따른 의무보험 등과의 관계

- 다른 법률에 따라 손해배상책임의 이행을 보장하는 보험 등에 가입하거나 준비금을 적립한 개인정보처리자는 「개인정보 보호법」에 따른 보험 등 가입 또는 준비금 적립 등의 조치를 아니할 수 있음

- ① 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.
- ② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 조치를 하지 아니할 수 있다.
 3. 다른 법률에 따라 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 개인정보처리자

(「개인정보 보호법」 제39조의7 제2항 제3호)

4

시정조치 명령 및 과태료

- 보험 등 가입이나 준비금 적립 등 손해배상책임 이행을 위하여 필요한 조치를 하지 않은 경우 : 시정조치 명령(미 이행시 과태료)

* 과태료 부과금액은 위반행위 횟수에 따라 차등 부과 (시행령 별표2 제2호 구목)

- ① 보호위원회는 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다.

1. 개인정보 침해행위의 중지
2. 개인정보 처리의 일시적인 정지
3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치

(「개인정보 보호법」 제64조 제1항)

- ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

27. 제64조제1항에 따른 시정조치 명령에 따르지 아니한 자

(「개인정보 보호법」 제75조 제2항)

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회이상 위반
구. 법 제64조제1항에 따른 시정조치 명령에 따르지 않은 경우	법 제75조 제2항 제27호	600	1,200	2,400

(「개인정보 보호법 시행령」 별표2)

5

시행일

- 손해배상책임 보장제도는 「정보통신망법」에서 2019년 6월 13일부터 시행되었고, 2020년 8월 5일부터 「개인정보 보호법」에 통합되었으며, 2024년 3월 15일부터 개인정보처리자 일반으로 확대 적용함

제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 삭제 <2015. 7. 24.>

③ 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 5배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다. <신설 2015. 7. 24., 2023. 3. 14.>

④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다. <신설 2015. 7. 24.>

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간·횟수 등
6. 개인정보처리자의 재산상태
7. 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[본조신설 2015. 7. 24.]

제39조의7(손해배상의 보장) ① 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다. <개정 2023. 3. 14.>

② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 조치를 하지 아니할 수 있다. <개정 2023. 3. 14.>

1. 대통령령으로 정하는 공공기관, 비영리법인 및 단체
2. 「소상공인기본법」 제2조제1항에 따른 소상공인으로서 대통령령으로 정하는 자에게 개인정보 처리를 위탁한 자
3. 다른 법률에 따라 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 개인정보처리자

③ 제1항 및 제2항에 따른 개인정보처리자의 손해배상책임 이행 기준 등에 필요한 사항은 대통령령으로 정한다. <신설 2023. 3. 14.>

[본조신설 2020. 2. 4.]

[제39조의9에서 이동, 종전 제39조의7은 삭제]

제48조의7(손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준 등) ① 법 제39조의7제1항에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 요건을 모두 갖춘 자(이하 “가입대상개인정보처리자”라 한다)를 말한다. <개정 2024. 3. 12.>

1. 전년도(법인의 경우에는 직전 사업연도를 말한다)의 매출액등이 10억원 이상일 것
2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 정보주체(제15조의3제2항제2호에 해당하는 정보주체는 제외한다. 이하 이 조에서 같다)의 수가 일일평균 1만명 이상일 것. 다만, 해당 연도에 영업의 전부 또는 일부의 양수, 분할·합병 등으로 개인정보를 이전받은 경우에는 이전받은 시점을 기준으로 정보주체의 수가 1만명 이상일 것

② 법 제39조의7제2항제1호에서 “대통령령으로 정하는 공공기관, 비영리법인 및 단체”란 다음 각 호의 기관을 말한다. <신설 2024. 3. 12.>

1. 공공기관. 다만, 제2조제2호부터 제5호까지에 해당하는 공공기관으로서 제32조제4항 각 호에 해당하는 공공기관은 제외한다.
2. 「공익법인의 설립·운영에 관한 법률」 제2조에 따른 공익법인
3. 「비영리민간단체 지원법」 제4조에 따라 등록한 단체

③ 법 제39조의7제2항제2호에서 “대통령령으로 정하는 자”란 다음 각 호의 요건을 모두 갖춘 자를 말한다. <개정 2024. 3. 12.>

1. 「소상공인기본법」 제2조제1항에 따른 소상공인으로부터 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리 업무를 위탁받은 자
2. 제1호에 따라 위탁받은 업무에 대하여 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 한 자

④ 가입대상개인정보처리자가 보험 또는 공제에 가입하거나 준비금을 적립할 경우 최저가입금액(준비금을 적립하는 경우 최소적립금액을 말한다. 이하 이 조에서 같다)의 기준은 별표 1의4와 같다. 다만, 가입대상개인정보처리자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우에는 보험 또는 공제 가입금액과 준비금 적립금액을 합산한 금액이 별표 1의4에서 정한 최저가입금액의 기준 이상이어야 한다. <개정 2023. 9. 12., 2024. 3. 12.>

[본조신설 2020. 8. 4.]

■ 개인정보 보호법 시행령 [별표 1의4] <개정 2024. 3. 12.>

손해배상책임의 이행을 위한 최저가입금액(최소적립금액)의 기준(제48조의7 제4항 관련)

가입대상개인정보처리자의 가입금액 산정요소		최저가입금액 (최소적립금액)
정보주체 수	매출액등	
100만명 이상	800억원 초과	10억원
	50억원 초과 800억원 이하	5억원
	10억원 이상 50억원 이하	2억원
10만명 이상 100만명 미만	800억원 초과	5억원
	50억원 초과 800억원 이하	2억원
	10억원 이상 50억원 이하	1억원
1만명 이상 10만명 미만	800억원 초과	2억원
	50억원 초과 800억원 이하	1억원
	10억원 이상 50억원 이하	5천만원

비고: 이 표에서 “매출액등”이란 제31조의2제1항제1호에 따른 매출액등을 말한다.

IV

FAQ (자주 묻는 질의답변)

1

적용 대상

Q1-1. 비영리기관이나 단체에 해당하는 학교, 병원 등도 보험 등 가입 또는 준비금 적립 적용 대상인지요?

- 「개인정보 보호법」 제39조의7에 따라 손해배상책임 이행을 위한 보험 가입 등의 적용 대상은 '개인정보처리자'이므로 매출액 등 및 개인정보 보유량 요건을 충족하는 비영리법인 및 기관·단체 등도 포함됩니다.
- 다만, 상기 요건을 충족하는 비영리법인이나 단체의 경우라도 「개인정보 보호법」 시행령 제48조의7 제2항에 따라 공익법인으로 허가된 법인이거나 비영리민간단체로 등록된 단체는 적용 대상에서 제외됩니다.

Q1-2. 위탁사(A사)를 대신하여 개인정보를 처리하는 수탁사(B)도 보험에 가입하거나 준비금을 적립해야 하는지요? 개인정보는 수탁사에 DB에 저장되고 위탁사는 접근 권한 등만 부여되고 있습니다.

- 「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)에서 개인정보 처리 위·수탁 관계에 대하여 규정하고 있으며,
- 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우, 위탁자가 보험 등 가입 또는 준비금 적립 적용 대상이고 수탁자는 적용 대상이 아닙니다.
- 다만, 수탁자가 고유업무 수행 등 독립적인 개인정보처리자의 지위에서 개인정보를 저장·관리하는 경우에는 적용 대상이 될 수 있습니다.

Q1-3. 소상공인이고 홈페이지 운영 및 개인정보 관리를 전문회사에 위탁하고 있는데, 이 경우 보험 가입 등의 의무가 면제될 수 있나요?

- 위탁자가 「소상공인기본법」 제2조 제1항에 따른 소상공인이고, 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리업무를 위탁받은 수탁자(예 : 클라우드 사업자, 호스팅 사업자 등)가 손해배상책임 이행을 위한 보험 가입 등을 하였을 경우, 위탁자는 적용 대상에서 제외될 수 있습니다.

Q1-4. 시행령 제48조의7 제3항 제1호에서 ‘소상공인으로부터 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리업무를 위탁받은 자’의 구체적 의미는 무엇인지요?

- 「개인정보 보호법 시행령」 제48조의7 제3항 제1호에서 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 않도록 하는 조치에 대한 구체적 기준을 제시하지는 않았으므로, 수탁자가 개인정보의 안전한 관리를 위해 자체적인 기술적·관리적 안전성 조치(예 : 내부관리계획 수립, 접속기록 보관 등)를 취하고 있다면 상기 규정에 따른 수탁자로 인정될 수 있을 것입니다.
- 이 경우 소상공인이 보험 가입 의무 등 적용 대상에서 제외되려면 위·수탁 계약 시 「시행령」 제48조의7 제3항에 따른 요건을 모두 충족하는 수탁사인지 확인해야 합니다.

Q1-5. 당사는 글로벌 기업의 한국 지사로 대부분의 주된 사업(서비스)은 글로벌 본사를 통해 이루어지는데, 이 경우 본사와 한국 지사 모두 보험 등에 가입해야 하는지요?

- 국내 정보 주체에게 해외 본사와 국내 지사가 각각 서비스를 제공하고 개인정보를 저장·이용하고 있다면 각각을 개인정보처리자로 보아 각각 보험 가입 등의 조치를 해야 합니다.
 - 만약 국내 이용자에게 서비스를 제공하고 개인정보를 저장·이용하는 주체는 국내 지사이거나 정보주체의 개인정보를 해외 본사의 시스템에 저장·이용하고 있다면 이 경우에도 각각을 개인정보처리자로 보아 보험 가입 등의 조치를 해야 합니다.
 - 다만 해외 본사가 서비스 제공 및 개인정보 저장·이용을 전담하고 국내 지사는 영업 등 개인정보와 무관한 업무만 수행할 경우, 해외 본사만 보험 가입 등의 조치를 하면 됩니다.
- ※ 해외 본사가 국내 손해배상보험 가입 시 보장범위에 내국인을 포함하고 있는지, 담보지역이 국내에 한정되어 있는지 등 약관 확인 필요

Q1-6. 당사는 가맹사업을 하는 본사이고, 가맹점들을 통해 유입되는 고객의 개인정보를 본사가 관리하는 시스템을 통해 저장·관리하고 있으나 본사가 별도로 수집하는 개인정보는 없습니다. 이 경우 본사가 보험 가입 등의 조치를 해야 하는지요?

- 「개인정보 보호법」 제39조의7에 따른 손해배상책임 이행을 위한 보험 가입 등의 적용 대상은 '개인정보처리자'이며, 이 경우 본사와 가맹점을 각각 개인정보처리자로 보아 손해배상책임 이행을 위한 보험 가입 등의 조치 의무가 각각 발생한다고 볼 수 있습니다.
- 다만 본사와 가맹점의 매출액과 정보주체 수를 합산하여 최저가입금액을 산정하고, 본사와 가맹점 모두를 피보험자로 하여 본사가 대표로 보험에 가입하는 것은 가능할 것으로 판단됩니다.

Q1-7. 자회사도 손해배상책임 가입 또는 준비금 적립을 의무적으로 해야 하나요? 아니면 모회사가 대비한 경우에는 제외되나요?

- 의무 적용 대상은 '법인' 단위이므로 자회사와 모회사가 별도 법인인 경우에는 각각 보험 가입 또는 준비금 적립 의무가 있습니다.

2

정보주체 수

Q2-1. 시행령 제48조의7 제1항 제2호, “전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 정보주체 수가 일일평균 1만명 이상일 것”의 의미는 무엇인지요?

- 전년도말 기준 직전 3개월(10~12월)을 기준으로 저장·관리되고 있는 개인정보 수를 매일 산정하여 그 평균값을 구하는 것으로, 개인정보처리자가 저장·관리하고 있는 개인정보의 누적 보유량(기 보유 정보+새롭게 유입된 정보-삭제된 정보)을 측정하는 개념입니다.
- 이 경우, 직전년도를 기준으로 하는 것이 원칙이나, 직전년도 산정이 불가능하다면 전전년도를 기준으로 하는 것도 가능합니다.
- 일일 평균 정보 주체 수를 구하는 산식은 다음과 같습니다.

$$= 3개월간(10월, 11월, 12월) \text{ 전체 일일 정보 주체 수의 총합 } \div 92(\text{일})$$

Q2-2. 당사는 이벤트 목적으로 이름/전화번호/주소 등 개인정보를 간헐적으로 보관·사용하고 있는데도 '정보 주체 수'에 포함해야 하는지요?

- 개인정보의 보관기간과 무관하게 전년도말 기준 직전 3개월 간 파기하지 않고 저장하고 있는 개인정보는 '정보주체 수' 산정 시 포함됩니다.

Q2-3. 개인정보처리자가 보관하고 있는 회원정보 뿐만 아니라 비회원, 휴면회원, 탈퇴회원 정보도 '정보주체 수'에 포함해야 하는지요?

- '정보주체 수'와 '회원 수'는 일치하는 개념은 아닙니다.
 - 회원 여부와 관계없이 개인정보처리자가 업무를 목적으로 수집·저장하고 있다면 '정보주체 수'에 포함됩니다.
- 탈퇴회원 및 휴면회원의 정보를 저장·관리하고 있는 경우, 정보주체 수 산정 시 포함됩니다.

Q2-4. 당사는 B2B 서비스를 하면서 거래 상대 기업의 담당자 개인정보 등을 저장하고 있는데, 이 경우 '정보 주체 수'에 포함되는지요?

- 원칙적으로 법인(또는 단체)의 정보(법인명, 소재지, 대표전화 등)는 개인정보에 해당하지 않으나,
 - 법인(또는 단체)의 정보이면서 동시에 개인정보인 대표자·임원·인·업무 담당자의 성명, 주소, 개인 연락처 등은 개인정보로 취급될 수 있고,
 - 거래 상대 기업으로부터 개인정보를 수집하여 저장하고 있다면 개인정보처리자에 해당될 수 있다고 판단됩니다.
- 또한, B2B 서비스를 제공받는 거래 상대 기업의 담당직원이 귀사에서 제공하는 B2B 서비스를 이용하고 있다면 '정보주체'에 해당하므로 '정보주체 수'에 포함됩니다.

Q2-5. 당사는 이용자를 대상으로 무료서비스를 제공하는데, 이 경우에도 '정보 주체 수' 산정 시 포함해야 하는지요?

- 서비스의 유·무료 여부와 무관하게 개인정보처리자가 업무를 목적으로 수집한 정보주체의 개인정보는 '정보주체 수' 산정에 포함됩니다.

Q2-6. '임직원 수'도 '정보주체 수'에 포함되는지요?

- 「개인정보 보호법 시행령」 제48조의7 제1항 제2호에 따라 개인정보처리자가 업무 수행을 위해 그에 소속된 임직원의 개인정보를 처리한 경우에는 정보 주체 수 산정 시 제외됩니다.

Q2-7. 당사는 여러 서비스를 제공하는 회사로, 한 사람이 여러 개의 서비스를 구매하는 등 거래 건수가 발생할 때마다 개인정보가 수집되는데 이 경우 정보주체 수는 어떻게 산정해야 하는지요?

- 동일인은 중복을 제외하여 '정보주체 수'를 산정하면 되며,
 - 동일인 여부는 개인정보처리자가 합리적으로 추정하여 구분하되 입증책임은 해당 개인정보처리자에게 있습니다.

3

매출액

Q3-1. 여러 계열사에서 수집하는 개인정보를 당사의 개인정보처리시스템에 통합하여 저장·관리하고 있는데, 보험 가입 등의 조치 시 시스템을 운영하는 당사의 매출액을 기준으로 적용하면 되나요?

- 매출액은 개인정보처리자인 법인(기업)의 총 매출액을 의미하며, 당사의 시스템에 여러 법인(기업)의 개인정보가 저장·관리되고 있다면, 보험 가입 등의 조치 시 매출액은 모든 개인정보처리자를 기준으로 산정하여야 합니다.

Q3-2. '매출액'을 산정하지 않는 기관의 경우 매출액 기준을 어떻게 적용 하나요?

- 「법인세법」 제4조 제3항 제1호에 따라 수익사업으로 생긴 수입을 매출액으로 보아야 합니다.

4

준비금

Q4-1. 준비금을 적립하는 구체적인 방법은 어떻게 되는지요?

- 준비금은 임의적립금(자본계정)으로 적립하고 주주총회 결의 등을 통해 해당 임의적립금이 「개인정보 보호법」 제39조의9의 의무이행을 위한 것임을 명확히 하여야 합니다.

Q4-2. 준비금 적립은 주주총회가 개최되는 내년 3월 이후 가능한데, 한시적으로 '준비금'을 '충당금'으로 적립하여도 되는지요?

- 충당금 적립 또는 별도계좌 예치 등을 통해 손해배상책임을 이행할 수 있는 준비를 한 상태에서, 차기 주주총회에서 준비금을 적립하겠다는 계획을 마련한 후 대표이사 결재를 받아 이를 보관하고 있는 경우에는 주주총회가 개최되는 시점까지 준비금을 적립한 것으로 인정할 수 있을 것으로 판단됩니다. 다만 주주총회 개최 이후에는 준비금으로 적립해야 합니다.

Q4-3. 준비금을 적립(또는 보험가입)한 사실은 향후 어떻게 증빙하면 되는지요? 신고 또는 증빙서류를 별도로 제출해야 하는지요?

- 이행 여부에 대한 신고·보고 의무는 없으나, 향후 이행 점검 시 보험증권·회계장부·주주총회 의사록 등 증빙자료 제출을 요구할 수 있습니다.

5

보험 가입시기, 가입방법 등

Q5-1. 현재 '개인정보보호배상책임보험' (또는 '사이버종합배상보험')에 가입되어 있습니다. 이 경우 개인정보 보호법에 따른 의무를 준수하고 있다고 인정될 수 있는지요?

- 가입하신 보험상품의 약관(특별약관을 포함)의 '보상하는 손해'가 「개인정보 보호법」 제39조 및 제39조의2에 따른 손해배상책임을 담보(보상)하는지 여부를 보험사에 확인하실 필요가 있으며,
 - 「개인정보 보호법」에서 요구하는 보장범위에 미치지(충족하지) 못한 경우에는 기존 가입 보험에 특약을 추가하시거나 기존 보험상품 해지 후 요건에 맞는 새로운 보험상품(개인정보 보호법에서 정한 의무보험 등)에 가입하셔야 할 것으로 판단됩니다.

Q5-2. 당사는 금년에 다른 회사로부터 영업을 양수받으면서 해당 업무와 관련된 개인정보도 함께 이전받았는데, 이 경우 보험 가입 등의 조치 의무가 발생하나요?

- 「개인정보 보호법 시행령」 제48조의7 제1항의 요건 단서에 따라 당사에서 영업양수로 인해 개인정보를 이전받은 경우 이전받은 시점을 기준으로 의무가 발생하며 이전받은 시점에 저장·관리되고 있는 개인정보의 정보주체 수를 기준으로 보험 가입 등의 조치를 이행하여야 합니다.

Q5-3. 당사는 금년에 설립·창업하여 직전년도 매출액이나 이용자가 없습니다. 이 경우에도 올해 보험에 가입해야 하나요?

- 「개인정보 보호법」 제39조의7의 요건은 직전년도를 기준으로 하므로, 금년도에는 가입하실 필요가 없으며, 법령상 기준이 충족되는 시점에 가입하시면 됩니다.

Q5-4. 다른 계열사와 함께 단체로 보험에 가입하는 경우 개정안에 따라 보험에 가입하였다고 볼 수 있는지요?

- 원칙적으로 준수 의무는 손해배상책임의 귀속 주체인 개별 법인(또는 자연인) 단위로 발생합니다.
- 단체보험을 통한 가입 형태도 무방하나 법령상 최저가입금액(보상한도액) 기준은 개별 기업별로 적용되므로, 단체보험의 최저가입금액은 개별 기업별로 준수해야 하는 가입금액을 합산한 금액이 되어야 합니다.

Q5-5. 글로벌 기업의 한국지사입니다. 해외에 소재한 보험사의 상품에 가입하는 것도 무방한지요?

- 「보험업법」 제3조에 따라 외국보험회사와 계약체결이 허용되는 선박, 항공 등 일부 보험상품, 국내에 취급되지 않는 보험종목 등을 제외하고는 해외 소재 보험회사의 상품에 가입하는 것은 불가능하나,
- 3개 이상의 국내보험회사로부터 가입이 거절되는 경우 등은 손해보험협회 확인 등을 거쳐 외국보험회사의 상품에 가입이 가능하며,
- 이 경우, 해당 상품이 「개인정보 보호법」 제39조 및 제39조의2에 따른 손해배상 책임을 보장하는지 입증할 수 있어야 합니다.

Q5-6. 휴업하거나 폐업한 경우에도 보험 등을 유지해야 하는지요?

- 폐업한 경우에는 보유하고 있던 개인정보를 모두 파기하였다면 보험 가입 등 의무 적용 제외가 가능합니다.
- 휴업한 경우에는 보유하고 있던 개인정보를 모두 파기하였다면 보험 가입 등 의무 적용 제외가 가능하지만, 법령에서 정한 기준 이상의 개인정보(1만명 이상)를 보유하고 있고 매출액(10억원 이상)이 발생하는 경우라면 보험 가입 등 의무 적용 대상이 됩니다.

Q5-7. 보험 가입과 준비금 적립을 병행하는 것은 가능한지요?

- 보험 가입과 준비금 적립은 병행 가능합니다. 이 경우 보험 가입금액과 준비금 적립 금액을 합산한 금액은 법령에서 정한 최저가입금액 기준을 충족해야 합니다.

Q5-8. 손해배상책임보험에 가입하더라도 법원의 확정판결이 아니면 보험금 청구가 되지 않는 것으로 알고 있는데, 분쟁조정 등 민사상 합의에 따른 배상금 지급 등의 경우에는 보험금을 청구할 수 없는지요?

- 반드시 법원의 확정판결이 있어야만 손해배상책임보험의 보험금을 청구할 수 있는 것은 아닙니다. 법원의 확정판결 외에도 분쟁조정위원회의 분쟁조정의 결과 등 민사상 합의에 따라 법상 손해배상책임이 인정되는 경우, 보험금을 청구할 수 있습니다.
- 다만, 보험사는 보험약관에 따라 손해액 산정 등의 절차를 거치게 되므로 청구액(민사상 합의된 배상금 등)과 약관 및 보험조건에 따른 보험금 지급여부 또는 지급 보험금이 상이할 수 있습니다.

Q6-1. 시행령 제48조의7 제3항, “다른 법률에 따라 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 것으로 본다” 규정의 구체적인 적용 사례를 알고 싶습니다.

- 「신용정보법」 제43조의3에 따른 의무보험(공제)에 가입했거나 준비금을 적립한 경우, 그 보장 내용이 「개인정보 보호법」 제39조 및 제39조의2에 따른 손해배상책임의 이행에 대한 부분까지 포함되었다면 「개인정보 보호법」 제39조의9(손해배상의 보장)에서 정한 의무를 충족할 때 동 규정을 준수한 것으로 판단됩니다.
- 이 경우에도 「개인정보 보호법」에서 정한 최저가입금액 기준 또는 최소적립금액 기준은 준수할 필요가 있습니다.

Q6-2. 당사는 모바일지급결제서비스업자로서, 전자금융거래법에 따른 ‘전자금융거래배상책임보험’ 및 ‘개인정보유출 배상책임 특별약관’에도 가입되어 있습니다. 이 경우 기존에 가입한 보험으로도 법상 의무를 충족한 것으로 볼 수 있는지요?

- 「전자금융거래법」 상 전자금융거래배상책임보험은 일반적으로 개인정보 유출에 따른 손해배상책임을 보장하고 있지 않아, 「개인정보 보호법」에서 정한 손해배상책임 범위를 충족하고 있지 않습니다.
- 다만, 기존에 판매되고 있는 ‘개인정보유출 배상책임 특별약관’에 가입하신 경우에는 해당 약관의 ‘보상하는 손해’가 「개인정보 보호법」 제39조 및 제39조의2에 따른 손해배상책임을 담보(보상)하는지 여부를 보험사에 확인하실 필요가 있습니다.
- 보장범위를 충족하지 않는다면, 「개인정보 보호법」에서 정한 의무보험 가입이 필요합니다.

일반 기준	①전년도 매출액등이 10억원 이상 + ②정보주체 수 1만명 이상 모두 충족	
	[적용 제외(의무면제)]	[적용(의무대상)]*
1. 공공기관 ※ 영 제32조제4항에 따라 <u>CPO 지정시 자격요건 의무대상 공공기관*</u> 은 제외		<p>○ CPO 지정시 자격요건 의무대상인 공공기관은 손해배상책임 보장 의무적용 대상임</p> <p>- 시행령 제2조제2호부터 제5호까지에 해당하는 공공기관으로서 <u>시행령 제32조제4항 각 호에</u> 해당하는 공공기관은 적용대상에 포함됨</p> <p><시행령 제32조제4항 각 호></p> <div style="border: 1px dotted black; padding: 5px;"> <p>1. 연간 매출액등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자(제2조제5호에 따른 각급 학교 및 「의료법」 제3조에 따른 의료기관은 제외한다)</p> <p>가. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자</p> <p>나. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자</p> <p>2. 직전 연도 12월 31일 기준으로 재학생 수(대학원 재학생 수를 포함한다)가 2만명 이상인 「고등교육법」 제2조에 따른 학교</p> <p>3. 「의료법」 제3조의4에 따른 상급종합병원</p> <p>4. 공공시스템운영기관</p> </div>
2. 공익법인의 설립·운영에 관한 법률 제2조에 따른 <u>공익법인</u>		
3. <u>비영리민간단체 지원법</u> 제4조에 따라 등록된 단체		
4. 다음 각호의 요건을 모두 갖춘 자에게 <u>개인정보 처리를 위탁한 「소상공인기본법」 제2조제1항에 따른 소상공인</u> 1) 「소상공인기본법」 제2조제1항에 따른 소상공인으로부터 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 <u>개인정보의 저장·관리 업무를 위탁받은 자</u> 2) 제1호에 따라 위탁받은 업무에 대하여 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 한 자		
5. <u>다른 법률</u> 에 따라 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 개인정보처리자		

* 일반조건(매출액 1억원 이상 + 정보주체 수 1만건 이상)을 충족하는 경우에 한함

회 사 명	연 락 처	콜센터 등 연락처	비 고
AIG손해보험	02-6210-6444		
DB손해보험	1588-0100		
KB손해보험	02-6900-3057	1544-0114	
MG손해보험	02-3788-2659	1588-5959	
NH농협손해보험	02-3786-7674	1644-9000	
SGI서울보증보험	1670-7000		
롯데손해보험	02-3455-3105	1588-3344	
메리츠화재해상보험	02-6464-3183	1566-7711	
삼성화재해상보험	1588-5114		
신한EZ손해보험	1544-2580		
에이스손해보험	02-6711-5801	1566-5800	
캐롯손해보험	1566-0300		
하나손해보험	02-6670-8925		
한화손해보험	1566-8000		
현대해상화재보험	1588-5656		
흥국화재해상보험	02-2002-6816	1688-1688	

* 소프트웨어공제조합 : 02-2142-7852~3

발 행 일 2024년 3월
발 행 처 개인정보보호위원회
지원기관 한국인터넷진흥원
디 자 인 호정씨앤피(☎02-2277-4718)



여성기업

※ 최신자료는 “개인정보보호위원회 누리집(pipc.go.kr)”, “개인정보 포털(privacy.go.kr)”에서 확인할 수 있습니다.

개인정보 손해배상책임 보장제도 안내서



개인정보보호위원회
Personal Information Protection Commission