

개인정보 처리 현황 점검 의무화 정책 자료

2026년 8월

개인정보 정책연구원

※ 이 문서는 교육·실습용으로 지어낸 가상의 자료입니다. 실재하는 법령이나 정부 발간물이 아닙니다.

목 차

제1장 총칙 및 의무 사항	3
제2장 제도 도입 배경	20
제3장 국내 실태조사 결과	39
제4장 해외 사례	45
제5장 이행 지원 방안	61
제6장 감독 및 제재	71
부칙	77
별표 · 서식	80

일러두기

이 자료는 개인정보 처리 현황 점검 의무화 제도의 내용을 조문과 해설로 정리한 것입니다. 조문은 제1장과 제6장에, 배경과 참고 자료는 제2장부터 제5장에 실었습니다.

제1장 총칙 및 의무 사항

제1절 개관

이 장은 개인정보 처리 현황 점검 의무화 제도의 뼈대를 담는다. 시행 시기와 적용 대상을 먼저 밝히고, 사업자가 지켜야 할 의무를 조문으로 적는다.

제도의 취지는 간명하다. 개인정보를 다루는 자가 스스로 자기 처리 현황을 정기적으로 들여다보고, 그 사실을 기록으로 남기게 하는 것이다. 사고가 난 뒤에 조사하는 방식으로는 늦다는 판단이 그 바탕에 있다.

제1장의 구성은 다음과 같다. 제1절은 개관, 제2절은 정의와 적용 범위, 제3절은 사업자의 의무다. 시행에 관한 사항은 부칙에 따로 두었고, 그 요지를 다음 쪽에 옮겨 적었다.

제2절 시행에 관한 사항

부칙 제1조(시행일)

이 제도는 2027년 1월 1일부터 시행한다.

시행일은 공포 후 준비에 필요한 기간을 고려하여 정하였다. 시행일 이전에 이루어진 개인정보 처리에 대하여는 종전의 기준을 적용한다.

시행일 이후 최초로 도래하는 점검 주기는 시행일이 속한 연도를 기준으로 산정한다. 다만 시행일 이후 6개월 이내에 점검을 마친 경우에는 해당 연도의 점검을 이행한 것으로 본다.

시행일과 관련한 세부 사항은 제6장 및 부칙에서 다시 다룬다.

부칙 제2조(적용의 유예)

상시 근로자 50인 미만인 사업자에 대하여는 이 제도의 적용을 시행일부터 1년간 유예한다.

유예 대상 여부는 시행일이 속한 달의 말일을 기준으로 판단한다. 유예 기간 중 상시 근로자가 50인 이상이 된 경우에는 그 사유가 발생한 날이 속한 연도의 다음 연도부터 적용한다.

상시 근로자 수의 산정 방법은 별표 1에 따른다. 파견 근로자와 단시간 근로자의 산입 여부도 별표 1에서 정한다.

유예를 받는 사업자라 하더라도 제9조의 유출 통지·신고 의무는 유예되지 아니한다. 이 점은 실무에서 자주 오해되는 대목이다.

제3절 정의

제2조(정의) 이 자료에서 쓰는 말의 뜻은 다음과 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 그 개인을 알아볼 수 있는 것을 말한다.
2. "처리"란 개인정보의 수집·생성·기록·저장·보유·가공·편집·검색·출력·정정·복구·이용·제공·공개·파기, 그 밖에 이와 유사한 행위를 말한다.
3. "처리 현황"이란 어떤 개인정보를 어떤 목적으로 어디에 두고 누가 다루는지에 관한 사실 관계를 말한다.
4. "점검"이란 처리 현황을 조사하여 기준에 맞는지 확인하고 그 결과를 기록하는 일련의 행위를 말한다.
5. "수탁자"란 개인정보의 처리 업무를 위탁받아 처리하는 자를 말한다.

제4절 적용 대상

제3조(적용 대상)

이 제도는 개인정보를 처리하는 모든 사업자에게 적용한다. 업종·규모·처리하는 개인정보의 양을 가리지 아니한다.

따라서 개인정보를 다루지 않는 사업자만이 적용 대상에서 벗어난다. 다만 임직원의 인사·급여 정보를 다루는 것만으로도 개인정보를 처리하는 것이므로, 실제로 적용을 받지 않는 사업자는 드물다.

공공기관에 대하여는 별도의 지침에 따른다. 이 자료에서 공공기관은 다루지 아니한다.

적용 대상이더라도 규모에 따라 시행 시기가 다를 수 있다. 부칙 제2조의 유예 규정을 함께 보아야 한다.

제5절 다른 기준과의 관계

제4조(다른 기준과의 관계) 개인정보 보호에 관하여 다른 기준에 특별한 규정이 있는 경우에는 그 기준에 따른다.

이 제도는 기존의 개인정보 보호 의무를 대체하지 아니한다. 기존 의무 위에 "정기적으로 확인하고 기록으로 남기는" 절차를 얹는 것으로 이해하는 것이 정확하다.

이미 정보보호 관리체계 인증을 받은 사업자는 인증 심사에서 확인된 사항의 범위에서 제7조의 점검을 갈음할 수 있다. 갈음의 범위는 별표 2에서 정한다.

제5조(사업자의 책무)

사업자는 개인정보를 처리할 때 정보주체의 권리가 침해되지 아니하도록 하여야 한다. 이를 위하여 처리 현황을 스스로 파악하고 관리하여야 한다.

제6조(책임자의 지정)

사업자는 개인정보 처리에 관한 업무를 총괄하는 책임자를 지정하여야 한다. 책임자는 제7조의 점검을 주관하고 그 결과를 대표자에게 보고한다.

책임자를 따로 두기 어려운 소규모 사업자의 경우에는 대표자가 책임자를 겸할 수 있다.

제6조의2(기본계획)

정책 소관 기관은 3년마다 개인정보 처리 현황 점검에 관한 기본계획을 세운다. 기본계획에는 다음 사항이 담긴다.

1. 점검 기준의 개선에 관한 사항
2. 사업자 지원에 관한 사항
3. 실태조사의 시기와 방법
4. 그 밖에 제도 운영에 필요한 사항

기본계획의 내용과 추진 실적은 매년 공개한다.

제6절 사업자의 의무

이 절은 사업자가 지켜야 할 의무를 정한다. 의무는 셋이다. 처리 현황의 정기 점검과 기록 보관, 위탁 계약의 필수 기재, 그리고 유출 시의 통지와 신고다.

세 의무는 서로 독립적이다. 하나를 지켰다고 하여 다른 하나가 면제되지 아니한다. 각 의무의 조문은 다음 쪽부터 차례로 싣는다.

의무의 이행 여부는 기록으로 확인한다. 이행하였으나 기록이 없는 경우, 감독 과정에서 이행 사실을 입증하기 어렵다는 점에 유의하여야 한다.

제7조(처리 현황의 점검 및 기록 보관)

- ① 사업자는 개인정보 처리 현황을 연 1회 이상 점검하여야 한다.
- ② 사업자는 점검의 결과를 기록하고, 그 기록을 3년간 보관하여야 한다.
- ③ 점검의 시기는 사업자가 정한다. 다만 한 번 정한 시기는 특별한 사유가 없으면 바꾸지 아니한다.
- ④ 점검 결과 기준에 맞지 아니한 사항이 확인된 경우에는 그 사항과 조치 내용을 함께 기록하여야 한다.

이 조가 이 제도의 핵심이다. 점검을 하였다는 사실보다, 무엇을 어떻게 보았고 무엇이 나왔는지를 남기는 것이 요구된다.

제7조 해설 — 점검 항목

점검에서 확인하여야 할 항목은 다음과 같다. 상세 서식은 별표 3에 있다.

1. 수집하고 있는 개인정보의 종류와 항목
2. 수집 목적과 보유 기간
3. 저장 위치와 접근 권한자
4. 제3자 제공 및 위탁 현황
5. 보유 기간이 지난 개인정보의 파기 여부
6. 접근 기록의 보관 상태

항목별로 "확인함 / 확인하지 못함 / 해당 없음"을 적고, 확인하지 못한 항목은 그 사유를 적는다.

제7조 해설 — 기록의 방법

기록의 형식은 정하지 아니한다. 문서·전자파일 어느 쪽이든 무방하다. 다만 다음 네 가지는 반드시 드러나야 한다.

점검한 날짜 · 점검한 사람 · 점검한 범위 · 확인된 사항과 조치

점검 범위를 일부로 한정된 경우에는 무엇을 제외하였는지 적어야 한다. 범위를 밝히지 않은 기록은 이행 기록으로 인정되지 아니할 수 있다.

기록의 보관 기간 3년은 점검을 마친 날부터 센다.

제8조(위탁 시 계약서 기재 사항)

사업자가 개인정보의 처리 업무를 위탁하는 경우, 계약서에 다음 다섯 가지를 반드시 기재하여야 한다.

1. 위탁 업무의 목적과 범위
2. 재위탁 제한에 관한 사항
3. 개인정보의 안전성 확보 조치에 관한 사항
4. 수탁자에 대한 관리·감독에 관한 사항
5. 손해배상 등 책임에 관한 사항

다섯 항목 중 하나라도 빠진 계약은 이 조를 위반한 것으로 본다. 표현이 모호하여 의무를 지우지 못하는 경우도 같다.

제8조 해설 — 수탁자 관리·감독

관리·감독은 계약서에 적는 것으로 끝나지 아니한다. 위탁자는 수탁자가 개인정보를 안전하게 처리하는지 실제로 확인하여야 한다.

확인인의 주기와 방법은 계약서에 정한다. 정하지 아니한 경우에는 연 1회 이상 확인한 것으로 보기 어렵다.

확인인의 결과는 제7조의 점검 기록에 포함하여 보관할 수 있다.

제8조 해설 — 재위탁

수탁자가 위탁받은 업무를 다시 다른 자에게 맡기려면 위탁자의 동의를 받아야 한다. 계약서에 이 점을 적지 아니한 경우에도 동의 없는 재위탁은 허용되지 아니한다.

동의를 서면으로 받는 것을 원칙으로 한다. 전자문서도 서면으로 본다.

재위탁이 이루어진 경우, 위탁자의 관리·감독 의무는 재수탁자에게도 미친다.

제8조 해설 — 계약 종료 시의 처리

위탁 계약이 끝나면 수탁자는 보유한 개인정보를 파기하거나 위탁자에게 반환하여야 한다. 어느 쪽으로 할지는 계약서에 미리 정한다.

파기한 경우에는 그 사실을 위탁자에게 알리고 증빙을 남긴다. 증빙에는 파기한 날짜·범위·방법이 들어간다.

계약 종료 후 일정 기간 보관이 필요한 경우에는 그 근거와 기간을 계약서에 적어야 한다.

제9조(유출 시 통지 및 신고)

- ① 개인정보가 유출되었음을 알게 된 사업자는 지체 없이 정보주체에게 그 사실을 알려야 한다.
- ② 사업자는 유출을 알게 된 때부터 72시간 이내에 소관 기관에 신고하여야 한다.
- ③ 72시간 이내에 신고하기 어려운 사유가 있는 경우에는 그 사유와 함께 먼저 신고하고, 확인된 사항을 나중에 보완할 수 있다.
- ④ 유출의 규모가 작더라도 신고 의무는 면제되지 아니한다.

이 의무는 부칙 제2조의 유예를 받는 사업자에게도 적용된다.

제2장 제도 도입 배경

제2장 제1절

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제2장 제2절

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

제2장 제3절

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

제2장 제4절

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

제2장 제5절

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

제2장 제6절

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

제2장 제7절

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제2장 제8절

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

제2장 제9절

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

제2장 제10절

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

제2장 제11절

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

제2장 제12절

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

제2장 제13절

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제2장 제14절

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

제2장 제15절

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

제2장 제16절

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

제2장 제17절

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

제2장 제18절

다음 절에서는 그 판단의 근거가 된 자료를 차례로 살핀다.

그 결과 감독은 사고가 난 뒤에야 이루어졌다. 사고가 나기 전에 무엇이 잘못되어 있었는지는 사고 조사 과정에서야 드러났다.

이러한 상태는 규범을 어기려는 의도에서 비롯된 것이 아니었다. 대부분은 한 번 만들어 둔 것을 다시 들여다보지 않았기 때문에 생긴 것이었다.

제2장 제19절

제도 도입 이전의 상황을 먼저 본다. 개인정보 보호에 관한 규범은 오래전부터 있었으나, 그 이행 여부를 사업자가 스스로 확인하도록 하는 절차는 없었다.

실무에서 흔히 관찰된 것은 다음과 같다. 쓰지 않는 개인정보가 오래 남아 있고, 퇴사자의 접근 권한이 살아 있으며, 위탁 계약서가 몇 해 전 양식 그대로였다.

따라서 필요한 것은 새로운 금지가 아니라 정기적으로 들여다보게 하는 장치라는 판단에 이르렀다. 이것이 이 제도의 출발점이다.

제3장 국내 실태조사 결과

제3장 제1절

실태조사는 2025년 하반기에 이루어졌다. 표본은 업종과 규모를 나누어 뽑았고, 설문과 현장 확인을 함께 썼다.

조사 결과 응답 사업자의 상당수가 자기 조직이 어떤 개인정보를 보유하고 있는지 전체 목록을 갖고 있지 않았다.

규모가 작을수록 이러한 경향이 뚜렷하였다. 다만 규모가 큰 사업자라 하여 모두 충실한 것은 아니었다.

제3장 제2절

조사 결과 응답 사업자의 상당수가 자기 조직이 어떤 개인정보를 보유하고 있는지 전체 목록을 갖고 있지 않았다.

위탁 계약서를 보유한 사업자 중에서도, 계약서에 안전성 확보 조치에 관한 조항이 들어 있는 경우는 절반에 미치지 못하였다.

실태조사는 2025년 하반기에 이루어졌다. 표본은 업종과 규모를 나누어 뽑았고, 설문과 현장 확인을 함께 썼다.

제3장 제3절

위탁 계약서를 보유한 사업자 중에서도, 계약서에 안전성 확보 조치에 관한 조항이 들어 있는 경우는 절반에 미치지 못하였다.

규모가 작을수록 이러한 경향이 뚜렷하였다. 다만 규모가 큰 사업자라 하여 모두 충실한 것은 아니었다.

조사 결과 응답 사업자의 상당수가 자기 조직이 어떤 개인정보를 보유하고 있는지 전체 목록을 갖고 있지 않았다.

제3장 제4절

규모가 작을수록 이러한 경향이 뚜렷하였다. 다만 규모가 큰 사업자라 하여 모두 충실한 것은 아니었다.

실태조사는 2025년 하반기에 이루어졌다. 표본은 업종과 규모를 나누어 뽑았고, 설문과 현장 확인을 함께 썼다.

위탁 계약서를 보유한 사업자 중에서도, 계약서에 안전성 확보 조치에 관한 조항이 들어 있는 경우는 절반에 미치지 못하였다.

제3장 제5절

실태조사는 2025년 하반기에 이루어졌다. 표본은 업종과 규모를 나누어 뽑았고, 설문과 현장 확인을 함께 썼다.

조사 결과 응답 사업자의 상당수가 자기 조직이 어떤 개인정보를 보유하고 있는지 전체 목록을 갖고 있지 않았다.

규모가 작을수록 이러한 경향이 뚜렷하였다. 다만 규모가 큰 사업자라 하여 모두 충실한 것은 아니었다.

제3장 제6절

조사 결과 응답 사업자의 상당수가 자기 조직이 어떤 개인정보를 보유하고 있는지 전체 목록을 갖고 있지 않았다.

위탁 계약서를 보유한 사업자 중에서도, 계약서에 안전성 확보 조치에 관한 조항이 들어 있는 경우는 절반에 미치지 못하였다.

실태조사는 2025년 하반기에 이루어졌다. 표본은 업종과 규모를 나누어 뽑았고, 설문과 현장 확인을 함께 썼다.

제4장 해외 사례

제4장 제1절

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

제4장 제2절

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

제4장 제3절

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

제4장 제4절

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

제4장 제5절

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

제4장 제6절

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

제4장 제7절

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

제4장 제8절

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

제4장 제9절

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

제4장 제10절

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

제4장 제11절

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

제4장 제12절

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

제4장 제13절

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

제4장 제14절

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

제4장 제15절

제재의 방식은 나뉜다. 과징금을 매출액에 연동하는 방식과, 정액 구간을 두는 방식이 함께 쓰인다.

여러 나라가 정기적인 자체 점검과 기록 보관을 요구하고 있다. 점검의 주기는 대체로 1년이며, 기록의 보관 기간은 나라마다 다르다.

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

제4장 제16절

해외의 유사 제도를 살핀다. 이 장은 참고 자료이며, 우리 제도의 해석 근거는 아니다.

위탁 계약에 관한 필수 기재 사항을 법에 열거하는 방식도 널리 쓰인다. 열거되는 항목의 수는 나라마다 다르지만, 목적과 범위·안전 조치·재위탁·감독·책임의 다섯 갈래는 대체로 공통된다.

유출 신고의 기한을 72시간으로 정한 예가 많다. 기한의 기산점을 "알게 된 때"로 삼는 것도 공통적이다.

제5장 이행 지원 방안

제5장 제1절

이행을 돕기 위한 지원 방안을 정리한다.

첫째, 점검 서식과 예시를 배포한다. 별표 3의 서식을 그대로 쓸 수 있다.

둘째, 위탁 계약서 표준안을 제공한다. 제8조의 다섯 항목이 모두 들어간 문안이다.

제5장 제2절

첫째, 점검 서식과 예시를 배포한다. 별표 3의 서식을 그대로 쓸 수 있다.

둘째, 위탁 계약서 표준안을 제공한다. 제8조의 다섯 항목이 모두 들어간 문안이다.

셋째, 소규모 사업자를 위한 상담 창구를 둔다. 상담 내용은 감독 자료로 쓰지 아니한다.

제5장 제3절

둘째, 위탁 계약서 표준안을 제공한다. 제8조의 다섯 항목이 모두 들어간 문안이다.

셋째, 소규모 사업자를 위한 상담 창구를 둔다. 상담 내용은 감독 자료로 쓰지 아니한다.

넷째, 시행 첫해에는 계도를 우선한다. 계도의 범위와 기간은 따로 알린다.

제5장 제4절

셋째, 소규모 사업자를 위한 상담 창구를 둔다. 상담 내용은 감독 자료로 쓰지 아니한다.

넷째, 시행 첫해에는 계도를 우선한다. 계도의 범위와 기간은 따로 알린다.

이행을 돕기 위한 지원 방안을 정리한다.

제5장 제5절

넷째, 시행 첫해에는 계도를 우선한다. 계도의 범위와 기간은 따로 알린다.

이행을 돕기 위한 지원 방안을 정리한다.

첫째, 점검 서식과 예시를 배포한다. 별표 3의 서식을 그대로 쓸 수 있다.

제5장 제6절

이행을 돕기 위한 지원 방안을 정리한다.

첫째, 점검 서식과 예시를 배포한다. 별표 3의 서식을 그대로 쓸 수 있다.

둘째, 위탁 계약서 표준안을 제공한다. 제8조의 다섯 항목이 모두 들어간 문안이다.

제5장 제7절

첫째, 점검 서식과 예시를 배포한다. 별표 3의 서식을 그대로 쓸 수 있다.

둘째, 위탁 계약서 표준안을 제공한다. 제8조의 다섯 항목이 모두 들어간 문안이다.

셋째, 소규모 사업자를 위한 상담 창구를 둔다. 상담 내용은 감독 자료로 쓰지 아니한다.

제5장 제8절

둘째, 위탁 계약서 표준안을 제공한다. 제8조의 다섯 항목이 모두 들어간 문안이다.

셋째, 소규모 사업자를 위한 상담 창구를 둔다. 상담 내용은 감독 자료로 쓰지 아니한다.

넷째, 시행 첫해에는 계도를 우선한다. 계도의 범위와 기간은 따로 알린다.

제5장 제9절

셋째, 소규모 사업자를 위한 상담 창구를 둔다. 상담 내용은 감독 자료로 쓰지 아니한다.

넷째, 시행 첫해에는 계도를 우선한다. 계도의 범위와 기간은 따로 알린다.

이행을 돕기 위한 지원 방안을 정리한다.

제5장 제10절

넷째, 시행 첫해에는 계도를 우선한다. 계도의 범위와 기간은 따로 알린다.

이행을 돕기 위한 지원 방안을 정리한다.

첫째, 점검 서식과 예시를 배포한다. 별표 3의 서식을 그대로 쓸 수 있다.

제6장 감독 및 제재

제33조(과태료)

① 다음 각 호의 어느 하나에 해당하는 자에게는 과태료를 부과한다.

1. 제7조를 위반하여 점검을 하지 아니하거나 기록을 보관하지 아니한 자
2. 제8조를 위반하여 필수 기재 사항을 빠뜨린 자
3. 제9조를 위반하여 기한 안에 신고하지 아니한 자

② 과태료의 금액 구간과 부과 기준은 시행령으로 정한다.

③ 과태료는 소관 기관이 부과·징수한다.

위반의 정도와 횟수, 시정 여부에 따라 감경할 수 있다. 감경의 사유와 한도 역시 시행령에서 정한다.

제6장 제2절 감독의 절차

감독은 서면 확인을 원칙으로 한다. 필요한 경우에 한하여 현장 확인을 한다.

시정 명령을 받은 사업자는 정한 기간 안에 이행하고 그 결과를 알려야 한다.

이의가 있는 경우에는 정해진 절차에 따라 다룰 수 있다.

제6장 제3절 감독의 절차

시정 명령을 받은 사업자는 정한 기간 안에 이행하고 그 결과를 알려야 한다.

이의가 있는 경우에는 정해진 절차에 따라 다룰 수 있다.

감독은 서면 확인을 원칙으로 한다. 필요한 경우에 한하여 현장 확인을 한다.

제6장 제4절 감독의 절차

이의가 있는 경우에는 정해진 절차에 따라 다룰 수 있다.

감독은 서면 확인을 원칙으로 한다. 필요한 경우에 한하여 현장 확인을 한다.

시정 명령을 받은 사업자는 정한 기간 안에 이행하고 그 결과를 알려야 한다.

제6장 제5절 감독의 절차

감독은 서면 확인을 원칙으로 한다. 필요한 경우에 한하여 현장 확인을 한다.

시정 명령을 받은 사업자는 정한 기간 안에 이행하고 그 결과를 알려야 한다.

이의가 있는 경우에는 정해진 절차에 따라 다룰 수 있다.

제6장 제6절 감독의 절차

시정 명령을 받은 사업자는 정한 기간 안에 이행하고 그 결과를 알려야 한다.

이의가 있는 경우에는 정해진 절차에 따라 다룰 수 있다.

감독은 서면 확인을 원칙으로 한다. 필요한 경우에 한하여 현장 확인을 한다.

부 칙

제1조(시행일) 이 제도는 2027년 1월 1일부터 시행한다.

제2조(적용의 유예) 상시 근로자 50인 미만인 사업자에 대하여는 시행일부터 1년간 적용을 유예한다.

제3조(경과 규정) 이 제도 시행 당시 이미 체결되어 있는 위탁 계약에 대하여는 그 계약의 갱신일 또는 시행일부터 1년이 되는 날 중 먼저 오는 날까지 종전의 예에 따를 수 있다.

제4조(경과 규정) 이 제도 시행 전에 이루어진 점검으로서 제7조의 요건을 갖춘 것은 이 제도에 따른 점검으로 본다.

제5조(다른 지침의 개정) 이 제도의 시행에 따라 관련 지침 중 해당 부분을 정비한다.

부칙 해설

경과 규정은 이미 맺어 둔 계약을 한꺼번에 바꾸지 않아도 되도록 한 것이다. 갱신 시점에 맞추어 정비하면 된다.

시행 전에 자체적으로 점검을 해 온 사업자는 그 기록을 그대로 쓸 수 있다. 다만 제7조가 요구하는 네 가지가 기록에 드러나야 한다.

[별표 1] 상시 근로자 수의 산정

상시 근로자 수는 직전 사업연도의 매월 말일 현재 근로자 수의 합을 개월 수로 나누어 산정한다.

파견 근로자는 산입하지 아니한다. 단시간 근로자는 근로시간에 비례하여 산입한다.

[별표 2] 인증 심사로 갈음할 수 있는 범위

정보보호 관리체계 인증 심사에서 확인된 항목은 제7조 점검 항목 중 해당 항목의 점검을 갈음할 수 있다.

갈음하는 경우에도 갈음의 근거가 되는 심사 결과를 점검 기록에 함께 보관하여야 한다.

[별표 3] 처리 현황 점검 기록 서식

점검일 / 점검자 / 점검 범위 / 제외한 범위와 사유

항목별 확인 결과 (확인함 · 확인하지 못함 · 해당 없음)

확인된 사항 / 조치 내용 / 조치 예정일

책임자 확인란

— 끝 —