개인정보 보호법 및 시행령 개정사항 안내

2023. 12. 29.

개인정보보호위원회

목 차

2023년 9월 15일 시행된 개정 개인정보 보호법에는 정보주체인 국민의 권리는 실질적으로 보장하면서 온라인-오프라인으로 이원화되어 있는 개인정보 처리 기준을 디지털 환경에 맞게 일원화하는 등 그동안 각계에서 논의되어 온 다양한 내용이 포함되어 있으며 주요 개정 내용은 다음과 같습니다.

첫째, 국민의 권익 보호가 보다 실질적으로 이루어질 수 있도록 정비하였습니다.

둘째, 영상정보·온-오프라인 이원화된 규제 등은 현장의 규제 개선 요청을 반영하여 영상정보처리기기 운영기준을 개선하고 모든 개인정보처리자에게 동일한 기준이 적용되도록 개선하였습니다.

셋째, 공공분야에서 개인정보가 안전하게 처리될 수 있도록 일정 규모 이상의 공공시스템에 대한 안전성 확보조치 의무 등을 강화하였습니다.

넷째, 글로벌 스탠다드를 반영하여 개인정보의 국외 이전 요건을 다양화하고 과징금 제도를 개편하였습니다.

안내서는 개인정보 보호법 개정에 따라 개인정보를 처리하는 과정에서 준수해야 할 사항에 많은 변화가 예상되어, 개정 취지를 설명하고 개인정보처리자가 유의해야 할 사항 등을 안내함으로써 제도의 안정적인 정착 및 수범자들의 이해도를 높이기 위한 목적으로 마련되었습니다.

안내서에 대한 자세한 사항은 개인정보보호위원회 개인정보보호정책과로 문의하여 주시기 바랍니다.

< 관련 제도 담당 부서 >

총괄, 동의·통지	개인정보보호정책과	02-2100-3055, 3057, 3047
과징금, 유출신고	조사총괄과	02-2100-3103
영상정보, 안전조치	신기술개인정보과	02-2100-3066, 3067
국외이전	국제협력담당관	02-2100-2482, 2485
분쟁조정	분쟁조정과	02-2100-3144
처리방침, 파일등록	자율보호정책과	02-2100-3050, 3080

1 개인정보 처리 관련 규정 개정

1 개인정보 수집·이용 및 제공

1. 개정 개요

□ 개인정보를 수집·이용 및 제공하는 요건이 정보통신서비스 제공자(온라인 사업자)와 공공기관·오프라인 등 개인정보처리자가 서로 다르게 규율되고 있어 개인정보 처리 요건을 일원화하면서 현장의 의견을 반영하여 일부 요건을 정비하였다.

○ 특히, 개인정보처리자가 개인정보를 수집·이용·제공하는 과정에서 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 없는 상태에서는 동의하도록 강제할 수 없도록 하되, 계약 이행 등과 같이 정보주체가 충분히 예상할 수 있는 합리적 범위 안에서는 개인정보를 수집·이용할 수 있도록 개선하였다.

□ 또한, 국민의 급박한 생명·신체·재산의 이익 보호, 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우와 같은 상황에서는 우선하여 개인정보를 수집·이용·제공할 수 있도록 하는 대신 안전조치·파기·정보주체의 권리 등의 규정은 준수하도록 하였다.

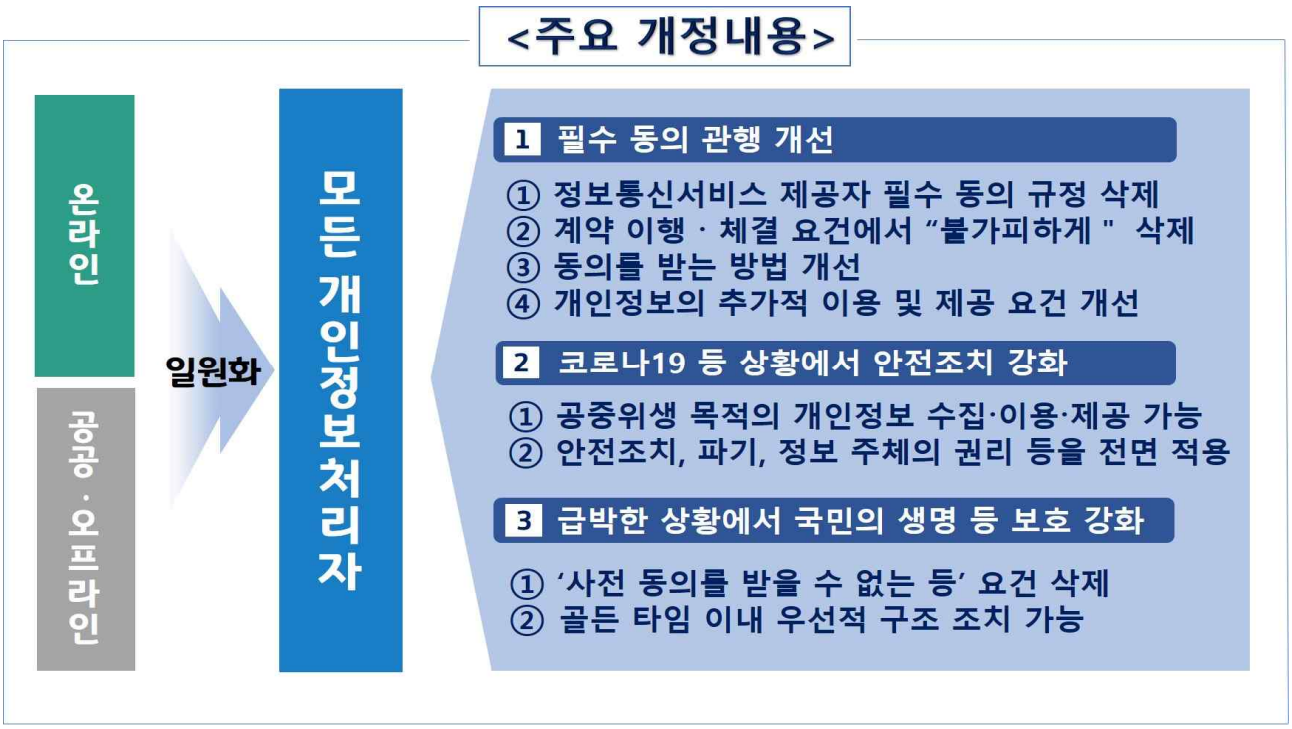
2. 개정 법령

법률	**제15조(개인정보의 수집·이용)** ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. 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. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우 5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다. 7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우 ② (생략) ③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.

	<특례 삭제> **제39조의3(개인정보의 수집·이용 동의 등에 대한 특례)** ① 정보통신서비스 제공자는 제15조제1항에도 불구하고 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다. 1. 개인정보의 수집·이용 목적 2. 수집하는 개인정보의 항목 3. 개인정보의 보유·이용 기간
	제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다. 1. 정보주체의 동의를 받은 경우 2. 제15조제1항제2호, 제3호 및 제5호부터 제7호까지에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우 ④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.
	제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제28조의8제1항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다. ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 규정에 따른 경우는 공공기관의 경우로 한정한다. 1. 정보주체로부터 별도의 동의를 받은 경우 2. 다른 법률에 특별한 규정이 있는 경우 3. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 4. 삭제 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 10. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우
	제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제22조의2제1항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다. 이 경우 다음 각 호의 경우에는 동의 사항을 구분하여 각각 동의를 받아야 한다. 1. 제15조제1항제1호에 따라 동의를 받는 경우 2. 제17조제1항제1호에 따라 동의를 받는 경우

	3. 제18조제2항제1호에 따라 동의를 받는 경우 4. 제19조제1호에 따라 동의를 받는 경우 5. 제23조제1항제1호에 따라 동의를 받는 경우 6. 제24조제1항제1호에 따라 동의를 받는 경우 7. 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 경우 8. 그 밖에 정보주체를 보호하기 위하여 동의 사항을 구분하여 동의를 받아야 할 필요가 있는 경우로서 대통령령으로 정하는 경우 ② 개인정보처리자는 제1항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다. ③ 개인정보처리자는 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 제30조제2항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다. ④ 삭제 <2023. 3. 14.> ⑤ 개인정보처리자는 정보주체가 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제1항제3호 및 제7호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다. ⑥ 삭제 <2023. 3. 14.> ⑦ 제1항부터 제5항까지에서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.
시행령	**제14조의2(개인정보의 추가적인 이용·제공의 기준 등)** ② 개인정보처리자는 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우에는 제1항 각 호의 고려사항에 대한 판단 기준을 법 제30조제1항에 따른 개인정보 처리방침에 공개하고, 법 제31조제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다.
	제17조(동의를 받는 방법) ① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 다음 각 호의 조건을 모두 충족해야 한다. 1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것 2. 동의를 받으려는 내용이 구체적이고 명확할 것 3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것 4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것 ② ~ ③ (생 략) ④ 개인정보처리자는 정보주체로부터 법 제22조제1항 각 호에 따른 동의를 받으려는 때에는 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게 알 수 있도록 표시해야 한다. ⑤ 법 제22조제3항 전단에서 "대통령령으로 정하는 방법"이란 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 "서면등의 방법"이라 한다)을 말한다.

3. 개정 내용



1 개인정보 수집·이용 요건 개선 (법 제15조)

1. 정보통신서비스 제공자의 경우에도 법 제15조 적용

□ 정보통신서비스 제공자*의 경우 종전 법 제39조의3에 따라 의무적으로 동의를 받아 왔으나 해당 규정이 삭제되었으므로 법 제15조의 규정을 따라야 한다.

○ 법 개정으로 모든 개인정보처리자는 법 제15조제1항 제1호부터 제7호까지의 사유 중 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있게 되었다.

* 인터넷 쇼핑·포털·온라인게임·소셜네트워크서비스(SNS) 등 온라인으로 서비스를 제공하는 자를 포함하며, 계약 등의 요건과 관계없이 의무적으로 동의를 받던 것을 개선

2. 개인정보 수집·이용 요건(제15조제1항) 변경[1] : 제1호, 제4호, 제5호, 제7호

□ 정보주체의 동의를 받은 경우 (제1호)

○ 개인정보처리자는 정보주체의 동의를 받은 경우에는 개인정보를 수집하여 이용할 수 있다. 개인정보처리자는 법 제15조제1항 제2호부터 제7호까지의 요건 중 어느 하나를 충족하는 경우 정보주체로부터 동의를 받지 않더라도 개인정보를 수집·이용할 수 있으므로 정보주체가 동의하지 않는다는 이유로 재화나 서비스 제공 자체를 거부하지 않아야 한다.

1) 법 제15조제1항 각 호 중 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위해 불가피한 경우(제2호), 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피한 경우(제3호), 개인정보처리자의 정당한 이익 달성을 위해 필요한 경우(제6호)의 요건은 종전의 규정을 유지함

□ **정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우 (제4호)**

○ 개인정보처리자와 정보주체 상호간 체결한 계약을 이행하거나 계약 체결을 위한 준비단계에서 정보주체의 요청에 따라 계약과 관련된 사실관계의 확인 등의 조치가 필요한 경우에는 정보주체로부터 별도의 동의 없이 개인정보를 수집하여 이용할 수 있다. 이 경우에도 계약이 체결되지 않은 경우에는 수집한 개인정보를 즉시 파기해야 한다. 다만, 계약이 체결되지 않은 경우에도 일정 기간 보유한다는 사실에 대한 동의를 받거나(제1호), 부정가입 시도 방지 등 개인정보처리자의 정당한 이익을 위하여 필요한 경우(제6호)에는 합리적인 기간 내에서 보유한 후 파기할 수 있다.

○ 종전에는 정보주체와의 계약 체결·이행을 위해 "불가피하게" 필요한 경우로 한정하였으나, 이번 개정을 통해 "불가피하게"를 삭제하여 개인정보처리자와 정보주체가 계약과 관련하여 서로 예상할 수 있는 합리적인 범위 내에서는 상호 신뢰에 기반하여 별도의 동의 없이도 개인정보를 수집하여 이용할 수 있도록 하였다.

<정보주체의 동의가 필요없는 계약 관련 사례>

사례1 정보주체와 체결한 계약을 이행하기 위해 필요한 경우

- 인터넷 쇼핑몰이 고객으로부터 구매상품 주문을 받아 결제-배송-AS 등 계약 이행을 위해 주소, 연락처, 결제정보 등을 수집하여 이용하는 경우
- 판매한 상품에 대한 AS 상담을 위해 전화한 고객의 성명, 연락처, 상품정보 등을 수집하여 이용하는 경우
- 회의 참석 전문가 등에게 참석수당을 지급하기 위해 이름, 계좌정보, 연락처 등을 수집하여 수당 지급에 이용하는 경우
- 백화점에서 상품구매 및 배송서비스를 위해 결제정보(카드정보 등)와 배송정보(주소, 연락처) 등 계약 이행을 위해 '불가피하게' 필요한 개인정보 외에 오배송 등 방지를 위해 이름, 이메일, 집전화번호, 배송희망시간 등의 개인정보를 수집하여 배송목적으로 이용하는 경우
- 아파트 관리사무소가 아파트 입주자와 아파트 관리서비스 계약 체결 및 이행을 위해 세대주 이름, 연락처, 차량번호 등 불가피하게 필요한 개인정보 외에 아파트 관리서비스 제공을 위해 필요한 범위 안애서 거주자수, 반려견 정보 등의 개인정보를 수집하여 이용하는 경우
- 맞춤형 추천이 계약의 본질적인 내용인 경우로서 서비스 이용계약에 따라 맞춤형 추천을 제공하기 위해 이용자의 검색기록 등을 수집하여 이용하는 경우
- 디지털 서비스 이용자 보호를 목적으로 보안위험, 악용사례(스팸, 멀웨어, 불법 콘텐츠 등) 등 감지 및 예방을 위해 서비스 이용계약에 따라 이용자의 개인정보를 수집하여 이용하는 경우

사례2 정보주체와 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우

- 인터넷서비스 이용을 위해 회원가입을 요청한 정보주체와의 이용계약 체결을 위해 이름, 연락처, 생성 아이디 등의 개인정보를 수집하는 경우

· 공인중개사가 부동산거래 중개 계약 체결을 위해 부동산 소유자, 권리관계 등을 미리 조사·확인하기 위해 개인정보를 수집하는 경우

· 회사가 취업지원자와 근로계약 체결 전에 지원자의 이력서, 졸업증명서, 성적증명서 등 정보를 수집·이용하는 경우

□ **명백히 정보주체 또는 제3자의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되는 경우 (제5호)**

○ 종전의 요건 중 '정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우'를 삭제하여, 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되면 국민의 생명 등 보호를 위해 우선하여 개인정보 수집·이용이 가능하도록 하였다.

□ **공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우 (제7호)**

○ 종전 법 제58조(적용의 일부 제외) 제1항제3호에서는 '공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보'의 경우에는 제3장부터 제7장까지를 적용하지 않도록 규정하고 있었다.

○ 코로나19 확산 상황에서 해당 개인정보가 안전조치, 파기, 정보주체의 권리 등 규정을 적용 배제함으로 인해 발생할 수 있는 부분에 대한 보완 필요성이 제기되었고, 이에 따라 법 제58조제1항제3호를 삭제하여 개인정보보호법이 적용되도록 하면서 '공중위생, 공공의 안전을 위해 긴급히 필요한 경우'에는 개인정보를 수집·이용 및 제공할 수 있도록 하였다.(법 제15조제1항, 제17조제1항, 제18조제2항의 사유에 추가하여 규정)

2 개인정보의 목적 범위 내 제공 요건 개선 (제17조)

□ 개인정보처리자가 정보주체의 개인정보를 제3자에게 제공할 수 있는 요건에 종전의 법 제15조제1항제2호, 제3호, 제5호 외에 제6호와 제7호를 추가하였다.

○ 이에 따라, 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우(제6호)와 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우(제7호)에는 그 목적 범위에서 개인정보를 제3자에게 제공할 수 있게 되었다.

3 개인정보의 목적 외 이용·제공 요건 개선 (제18조)

□ **모든 개인정보처리자에 대하여 동일 요건 적용 : 제18조제2항 단서**

○ 종전에는 정보통신서비스 제공자의 경우에는 정보주체로부터 별도의 동의를 받은 경우(제1호), 다른 법률에 특별한 규정이 있는 경우(제2호)에만 목적 외 이용·제공이 가능하도록 했던 제18조제2항단서 규정을 삭제하여 모든 개인정보처리자가 동일한 요건을 적용받도록 하였다.

※ 다만, 공공기관에만 적용되는 제5호부터 제9호까지의 요건은 유지

□ **개인정보의 목적 외 이용·제공 요건 개선 : 제18조제2항 제3호·제10호**

○ 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우(제3호)에는 동의 없이도 제3자에게 목적 외 이용·제공이 가능하도록 하였다. 종전에는 '정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서'와 같은 제약이 있었으나 이를 삭제하여 국민의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 판단되는 경우에는 우선 조치할 수 있도록 하였다.

사례 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 경우

· 렌터카 서비스 사업자가 아동 대상 범죄가 예상되는 급박한 상황에서 관계기관으로부터 구조를 위해 렌터카 서비스 이용자인 범죄자의 주소 등 정보를 제공해 줄 것을 요청받은 경우

· 재난, 실종 등 국민의 생명, 신체에 대한 위험이 급박한 상황에서 신속한 구조를 위해 CCTV 영상 등의 제공을 요청받은 경우 관계기관에 해당 정보를 우선하여 제공하는 경우

○ 또한, 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우(제10호)에도 목적 외로 이용·제공이 가능하도록 하였다. 다만, 이 경우에도 개인정보보호법에서 규정하고 있는 안전조치, 파기, 정보주체의 권리 보장 등의 조치는 이행하여야 한다.

사례 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

· 코로나19 등 감염병이 확산되는 상황에서는 정보주체의 별도의 동의 없이도 개인정보를 당초 수집한 목적 외로 이용하거나 제공할 수 있으나, 그 외 개인정보보호법 상 개인정보처리자가 준수해야 할 안전조치, 파기, 정보주체의 권리 보장 등의 의무는 모두 적용됨

4 개인정보를 추가적으로 이용·제공할 수 있는 경우

(법 제15조제3항·제17조제4항, 영 제14조의2)

□ 개인정보처리자는 정보주체의 동의 없이 개인정보를 이용 또는 제공하려는 경우에는 ①당초 수집 목적과 관련성이 있는지 여부, ②개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부, ③정보주체의 이익을 부당하게 침해하는지 여부, ④가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부를 고려하여 추가적인 이용 또는 제공을 할지 여부를 결정해야 한다.

□ 종전에는 고려사항에 대한 판단 기준을 개인정보 처리방침에 미리 공개하도록 하였으나, 개인정보의 추가적인 이용 또는 제공을 해야 하는 개별적인 상황을 미리 예측하여 공개하는 것이 어려운 점을 고려하여 '지속적으로 발생하는 경우'에 한하여 공개하도록 개선하였다.

□ 개인사업자와 정보주체를 연결해 주는 중개서비스(예: 오픈마켓)의 경우를 예로 들면,

○ 중개서비스의 경우에는 서비스 이용계약의 내용 안에 정보주체의 개인정보를 제3자(개인사업자)에게 제공해야만 배송 등 계약 이행이 가능한 상황이 전제되어 있으므로 해당 개인정보의 제공은 당초 수집 목적과 합리적으로 관련된 범위 안에 있다고 볼 수 있다.

○ 이 경우 ① 정보주체는 중개서비스 사업자와의 계약 과정에서 개인정보가 제3자에게 제공된다는 사실을 충분히 예측[2]할 수 있다는 점, ② 당사자 간 자유로운 의사에 따른 계약을 이행하기 위한 것이므로 정보주체의 이익을 부당하게 침해하지 않는다는 점, ③ 동의를 받도록 할 경우 동의하지 않으면 서비스 이용 자체가 불가능하게 되어 정보주체의 선택권을 오히려 제약할 수 있다는 점, ④ 서비스의 특성에 따라 다양한 침해 가능성을 적극적으로 고려하여 그에 맞는 안전성 확보에 필요한 조치(예: 택시 중개서비스에서의 안심번호)를 하는 것도 가능하다는 점 등을 고려하면, 중개사업자가 정보주체의 개인정보를 제3자에게 제공하는 것은 당초 개인정보를 수집한 목적과 관련된 범위 안에서 추가적으로 제공한 것으로 볼 수 있다.

○ 이 경우 중개서비스 이용계약의 이행과 관련되어 지속적으로 발생하는 경우에 해당하므로 개인정보 처리방침을 통해 고려사항에 대한 판단기준을 구체적으로 공개하고, 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다.

○ 다만, 해당 서비스의 본질적인 내용에 개인정보의 제공이 포함되어 있지 않아서 정보주체가 개인정보의 제공 사실과 제공받는 자 등을 예측하기 어려운 경우에는 목적 범위 내라고 하더라도 다른 동의와 구분하여 각각 동의를 받아야 한다.

사례 추가적인 이용·제공이 지속적으로 발생하는 경우

- 정보주체가 택시 중개서비스 앱을 이용하기 위하여 이용계약을 체결하고 해당 택시 중개서비스 앱 사업자가 정보주체의 요청에 따른 택시 호출을 위해 정보주체의 개인정보를 제3자인 택시기사에게 제공하는 경우
- 인터넷 쇼핑몰(오픈마켓) 사업자가 상품 중개서비스 계약 이행을 위해 수집한 정보주체의 개인정보를 해당 인터넷 쇼핑몰에 입점하고 있는 제3자인 상품 판매자에게 배송 등 계약 이행을 목적으로 제공하는 경우
- 통신판매중개플랫폼 사업자가 플랫폼 입점 사업자와 고객을 연결하는 플랫폼을 통해 플랫폼 이용자의 이름, 주소, 연락처, 주문내역, 결제 내역 등의 개인정보를 거래 확인 및 배송 등을 위한 목적으로 입점 사업자에게 제공하는 경우
- 통신과금서비스 제공자가 소액결제 등 휴대전화 결제 서비스를 제공하는 과정에서 서비스 이용 계약을 체결하고 통신과금서비스를 이용 중인 정보주체의 가입자식별정보, 결제일시·결제금액 등 결제내역정보를 결제 목적으로 이동통신사에 제공하는 경우

2) 중개서비스 사업자가 중개서비스 제공 과정에서 개인정보를 제공받는 제3자(개인사업자)에 대한 정보를 추가적으로 정보주체에게 고지하는 절차를 병행할 경우 추가적인 제공에 대한 예측 가능성을 높일 수 있음

· 인적자원(HR) 채용 플랫폼 사업자가 구직 지원 서비스를 제공하는 과정에서 정보주체가 입사 지원하는 기업에 정보주체의 이력정보 등을 제공하는 경우

사례 추가적인 이용·제공이 일회성으로 발생하는 경우

· 화장품을 판매한 소매점이 소비자(정보주체)의 동의를 받아 수집한 연락처 정보를 화장품 제조회사가 실시하는 소비자 보호 목적의 리콜 실시를 위해 화장품 제조회사에 제공하는 경우

· 고객이 가게에서 계산한 물건을 가져가지 않고 다른 고객이 실수로 그 물건을 가져간 경우 가게주인이 물건을 가져간 고객에게 연락하여 물건반환을 요청하기 위해 이용하는 경우

· 기업·기관 등이 근로자의 경력을 증명할 수 있는 근로와 관련된 개인정보를 적법하게 보유하고 있는 경우로서 근로자의 경력증명을 위하여 취업규칙에 명시된 경력증명서 발급기간이 경과한 후 근로자의 요청에 따라 경력증명서를 발급하기 위해 개인정보를 추가로 이용하는 경우

4. 개인정보처리자 유의사항

□ 개인정보처리자는 이 법에 따른 개인정보 처리에 대하여 정보주체로부터 동의를 받을 때에는 각각의 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다. 특히 아래 경우에는 동의 사항을 구분하여 각각 동의를 받아야 한다.

< 동의 사항을 구분하여 각각 동의를 받아야 하는 경우 >

1. 제15조제1항제1호에 따라 동의를 받는 경우
2. 제17조제1항제1호에 따라 동의를 받는 경우
3. 제18조제2항제1호에 따라 동의를 받는 경우
4. 제19조제1호에 따라 동의를 받는 경우
5. 제23조제1항제1호에 따라 동의를 받는 경우
6. 제24조제1항제1호에 따라 동의를 받는 경우
7. 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 경우
8. 그 밖에 정보주체를 보호하기 위하여 동의 사항을 구분하여 동의를 받아야 할 필요가 있는 경우로서 대통령령으로 정하는 경우

※ 근거 : 법 제22조(동의를 받는 방법) 제1항

□ 2024년 9월 15일부터는 정보주체로부터 개인정보 처리에 대한 동의를 받을 때에는 아래의 조건을 모두 충족해야 한다. 종전에도 판례를 통해 적용해 온 조건이나 시행령에 동의의 조건을 명확히 규정하였으며, 현장에서의 동의 절차를 개선할 준비 기간을 부여하기 위해 시행령 부칙 개정을 통해 시행일을 1년 유예하였다.

< 개인정보 처리에 대한 정보주체의 동의를 받을 때 충족해야 하는 조건 >

1. 정보주체의 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것

2. 동의를 받으려는 내용이 구체적이고 명확할 것

3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것

4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

※ 근거 : 영 제17조(동의를 받는 방법) 제1항, 영 부칙 제1조(시행일) 제1호

○ 정보주체로부터 개인정보 처리에 대한 동의를 받을 때에는 '정보주체의 자유로운 의사'에 따라 동의 여부를 결정할 수 있도록 동의 절차를 개편해야 한다. 동의하지 않으면 재화 공급 또는 서비스 제공 자체를 거부하는 방식으로 운영할 경우 정보주체의 자유로운 의사에 따른 동의 여부의 결정으로 보기 어렵다.

※ 동의하지 않을 경우에도 서비스 자체의 이용은 가능하나 정보주체의 자유로운 의사를 제약하지 않는 일부 부가서비스 이용을 제한하는 것은 가능함

□ 종전 정보통신서비스 제공자는 의무적으로 개인정보 수집·이용에 대한 동의를 받아왔으나, 법 개정으로 개인정보를 수집·이용하려면 법 제15조제1항 각 호의 사항 중 어느 하나의 요건에 해당해야 하는 방향으로 개정된 점에 유의해야 한다.

○ 특히, 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우에는 동의 없이 개인정보를 수집하여 이용할 수 있다.

□ 당초 수집 목적과 관련이 있고 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있으며 정보주체의 이익을 부당하게 침해하지 않는 경우에는 다양한 상황에 맞는 안전성 확보에 필요한 조치 여부를 고려한 후 개인정보를 추가적으로 이용 또는 제공할 수 있다.

○ 특히, 중개서비스와 같이 서비스 이용계약의 본질적인 내용이 개인정보의 제3자 제공을 포함하고 있는 경우에는 별도의 동의 없이 추가적으로 개인정보를 이용 또는 제공할 수 있는 점을 고려하여 개인정보 처리에 대한 적법요건을 검토해야 한다.

□ 개인정보처리자는 정보주체의 동의 없이 처리할 수 있는 개인정보에 대하여는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 공개하는 등의 조치를 해야 하며, 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담해야 한다는 점을 유의해야 한다.

□ 구조 등 업무를 수행하는 관계기관이 국민의 급박한 생명, 신체, 재산의 이익을 보호하기 위하여 개인정보의 이용 또는 제공을 요청하는 경우에는 골든타임 내 구조가 가능하도록 신속하게 조치하고, 개인정보 보호를 이유로 조치를 지연하거나 거부하는 사례가 발생하지 않도록 유의해야 한다.

◈ 기존의 '알기 쉬운 개인정보 처리 동의 안내서'('22.3월)와 '개인정보 처리 위·수탁 안내서'('20.12월)를 사례 중심으로 통합·보완하여 현장의 혼선이 없도록 추가로 안내할 예정임(~'24.상반기)

5. 제재 규정

위반행위	제재 내용
제15조제1항, 제17조제1항, 제18조제1항・제2항(제26조제8항에 따라 준용되는 경우를 포함한다) 또는 제19조를 위반하여 개인정보를 처리한 경우	과징금 (제64조의2제1항제1호)
정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알면서도 개인정보를 제공받은 자 (제17조제1항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제1호)
개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 (제18조제1항・제2항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제2호)

6. 질의 응답

□ 동의를 받을 때에는 정보주체의 자유로운 의사에 따르도록 하였는데, 앞으로는 개인정보를 수집하는 과정에서 필수적으로 동의를 요구해서는 안되는 것인지?

⇨ 동의를 받을 때에는 정보주체의 자유로운 의사에 따라 동의 여부를 결정할 수 있도록 해야 함. 따라서, 정보주체에게 동의를 요청하는 과정에서 동의를 거부할 경우 서비스 계약체결 자체를 거부하는 등의 방법으로 동의를 강제해서는 안 됨
시행령 제17조제1항의 해당 규정은 2024년 9월 15일부터 시행 예정이므로 정보주체의 자유로운 의사가 반영되도록 동의 절차를 개편하는 준비를 진행해야 함

⇨ 동의를 받지 않아도 되는 개인정보라는 입증책임은 개인정보처리자에게 있으므로 계약이행을 위해 필요한 개인정보인지, 개인정보의 추가적 이용・제공에 해당하여 동의가 필요 없는지 등을 확인하여 이에 해당하는 경우 불필요하게 동의를 요구하지 않아야 함

□ 현재 정보주체가 동의 여부를 선택할 수 있도록 동의절차를 운영 중인데, 선택동의는 현재처럼 계속 유지해도 되는지?

⇨ 선택동의는 계약 이행 등을 위해 필요하지 않은 정보에 대하여 개인정보처리자의 필요에 의해 수집·이용 동의를 요구하는 것이므로, 정보주체의 자유로운 의사에 따라 동의 여부를 결정할 수 있도록 하는 등의 조치를 한 경우라면 선택동의를 유지할 수 있음

다만, 선택적으로 동의할 수 있는 사항에 대한 동의를 받으려는 때에는 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게 확인할 수 있도록 다른 사항과 구분하여 표시하여야 함

□ 이용자의 개인정보나 관심사 등을 분석하여 서비스 내에서 맞춤형 콘텐츠를 추천하는 것도 재화·서비스 홍보나 판매 권유로 보아 별도 동의를 받아야 하는지?

⇨ 맞춤형 콘텐츠 추천이 계약의 본질적인 내용이며 해당 내용을 이용계약·약관 등에 명확히 규정하고 있고 정보주체가 충분히 알 수 있도록 조치하였다면, 계약 이행을 위해 별도의 동의 없이도 수집·이용할 수 있음

□ 「개인정보 처리 방법에 관한 고시」 제4조제1호 규정이 변경되었는데, 이제는 서면 동의 시 글씨 크기가 9포인트보다 작아도 되는지?

⇨ 해당 규정은 서면(전자문서 포함) 동의 시 중요한 내용의 표시 방법을 디지털 환경에 맞게 정비한 것으로, '9포인트 이상', '다른 내용보다 20퍼센트 이상 크게' 규정은 삭제되었으나 글씨의 크기, 색깔, 굵기 또는 밑줄 등을 통하여 그 내용을 명확히 표시하도록 하고 있음

⇨ 따라서, 해당 규정이 변경되었다 하더라도 글씨 크기를 의도적으로 작게 하는 등 정보주체를 기만하거나 알아보기 어려운 형태로 동의를 받아서는 안 됨

참고 개인정보 처리 방법에 관한 고시 ('23.10.16. 시행)

제1조(목적) 이 고시는 「개인정보 보호법」 제18조제4항·제22조제2항, 같은 법 시행령 제15조·제34조제1항·제41조제3항 및 제5항·제43조제3항·제44조제2항·제45조제2항에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(공공기관에 의한 개인정보의 목적 외 이용 또는 제3자 제공의 공고) 공공기관은 개인정보를 목적외의 용도로 이용하거나 제3자에게 제공(이하 "목적외이용등"이라 한다)하는 경우에는 「개인정보 보호법」(이하 "법"이라 한다) 제18조제4항에 따라 개인정보를 목적외이용등을 한 날부터 30일 이내에 다음 각 호의 사항을 관보 또는 인터넷 홈페이지에 게재하여야 한다. 이 경우 인터넷 홈페이지에 게재할 때에는 10일 이상 계속 게재하여야 한다.

1. 목적외이용등을 한 날짜
2. 목적외이용등의 법적 근거
3. 목적외이용등의 목적
4. 목적외이용등을 한 개인정보의 항목(구성)

제3조(개인정보 보호업무 관련 장부 및 문서 서식) ① 법 제18조제2항과 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제15조에 따른 개인정보의 목적 외 이용 및 제3자 제공 대장은 별지 제1호서식과 같다.

② 법 제32조제1항과 영 제34조제1항에 따른 개인정보파일 등록 신청 및 변경등록 신청은 별지 제2호서식의 개인정보파일 등록·변경등록 신청서에 따른다.

③ 법 제35조제2항과 영 제41조제3항에 따른 개인정보 열람의 요구는 별지 제8호서식의 개인정보 열람 요구서에 따른다.

④ 법 제35조제5항과 영 제41조제5항에 따른 개인정보 열람 및 일부열람의 통지, 법 제35조제3항 후단과 영 제42조제2항에 따른 개인정보 열람연기의 통지, 법 제35조제4항과 영 제42조제2항에 따른 열람거절의 통지는 별지 제9호서식의 개인정보 열람, 일부열람, 열람연기, 열람거절 통지서에 따른다.

⑤ 법 제36조제6항과 영 제43조제3항에 따른 개인정보 정정·삭제 요구에 대한 결과의 통지, 법 제37조제6항과 영 제44조제2항에 따른 개인정보 처리정지 요구에 대한 결과의 통지는 별지 제10호서식의 개인정보 정정·삭제, 처리정지 요구에 대한 결과 통지서에 따른다.

⑥ 영 제45조제2항에 따른 정보주체의 위임장은 별지 제11호서식과 같다.

제4조(서면 동의 시 중요한 내용의 표시 방법) 법 제22조제2항에서 "보호위원회가 고시로 정하는 방법"이란 다음 각 호의 방법을 통해 종이 인쇄물, 컴퓨터 표시화면 등 서면 동의를 요구하는 매체의 특성과 정보주체의 이용환경 등을 고려하여 정보주체가 쉽게 알아볼 수 있도록 표시하는 방법을 말한다.

1. 글씨의 크기, 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
2. 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

부칙 <제2023-12호, 2023. 10. 16.>

이 고시는 공포한 날부터 시행한다.

※ 별지 서식은 국가법령정보센터(www.law.go.kr) 참조

※ 종전 별지 제3호부터 제7호 서식은 「개인정보 영향평가에 관한 고시」로 위치 이동

② 개인정보 처리방침 평가 (법 제30조의2)

1. 개정 개요

□ 개인정보 보호법은 개인정보처리자를 대상으로 개인정보 처리방침 작성 및 공개 의무를 부과하고 있으나,

○ 처리방침의 내용의 적정성에 대한 판단 기준이 모호하며, 대부분의 처리방침이 획일적이고, 텍스트 나열 등으로 인해 정보주체가 이해하기 어려워 정보주체가 처리방침을 확인하지 않는 등의 문제가 발생하였다.

* 개인정보 처리방침을 확인하는 정보주체는 37.5%에 불과하며, 미확인 사유로는 '읽어야 할 내용이 많고 이해하기 어려워서'가 47.7%로 가장 높게 나타남(2022 개인정보보호 및 활용조사)

□ 이에, 보호위원회가 개인정보 처리방침의 적정성, 가독성, 접근성 등을 평가하여 개인정보 처리의 책임성, 투명성을 높일 수 있도록 개인정보 처리방침 평가 제도를 도입하였다.

2. 개정 법령

법률	**제30조의2(개인정보 처리방침의 평가 및 개선권고)** ① 보호위원회는 개인정보 처리방침에 관하여 다음 각 호의 사항을 평가하고, 평가 결과 개선이 필요하다고 인정하는 경우에는 개인정보처리자에게 제61조제2항에 따라 개선을 권고할 수 있다. 1. 이 법에 따라 개인정보 처리방침에 포함하여야 할 사항을 적정하게 정하고 있는지 여부 2. 개인정보 처리방침을 알기 쉽게 작성하였는지 여부 3. 개인정보 처리방침을 정보주체가 쉽게 확인할 수 있는 방법으로 공개하고 있는지 여부 ② 개인정보 처리방침의 평가 대상, 기준 및 절차 등에 필요한 사항은 대통령령으로 정한다.
시행령	**제31조의2(개인정보 처리방침의 평가 대상 및 절차)** ① 보호위원회는 법 제30조의2제1항에 따라 개인정보 처리방침을 평가하는 경우 다음 각 호의 사항을 종합적으로 고려하여 평가 대상을 선정한다. 1. 개인정보처리자의 유형 및 매출액 규모 2. 민감정보 및 고유식별정보 등 처리하는 개인정보의 유형 및 규모 3. 개인정보 처리의 법적 근거 및 방식 4. 법 위반행위 발생 여부 5. 아동·청소년 등 정보주체의 특성 ② 보호위원회는 제1항에 따라 평가 대상 개인정보 처리방침을 선정한 경우에는 평가 개시 10일 전까지 해당 개인정보처리자에게 평가 내용·일정 및 절차 등이 포함된 평가계획을 통보해야 한다. ③ 보호위원회는 법 제30조의2에 따른 개인정보 처리방침의 평가에 필요한 경우에는 해당 개인정보처리자에게 의견을 제출하도록 요청할 수 있다. ④ 보호위원회는 법 제30조의2에 따라 개인정보 처리방침을 평가한 후 그 결과를 지체 없이 해당 개인정보처리자에게 통보해야 한다. ⑤ 제1항부터 제4항까지에서 규정한 사항 외에 개인정보 처리방침 평가를 위한 세부적인 대상 선정 기준과 절차는 보호위원회가 정하여 고시한다.

3. 개정 내용

□ 개인정보처리자가 수립·공개하고 있는 개인정보 처리방침에 대해 보호위원회가 내용의 적정성, 이해의 용이성, 접근성 등을 평가할 수 있도록 개정하였다.

□ 평가 대상은 개인정보처리자의 유형 및 매출액, 처리하는 개인정보의 유형 및 규모, 개인정보 처리의 법적 근거 및 방식, 법 위반행위 발생 여부, 아동·청소년 등 정보주체의 특성 등을 종합적으로 고려하여 보호위원회가 선정할 계획이다.

○ 이 중 '개인정보처리자의 유형 및 매출액'(영 제31조의2 제1항 제1호)과 '개인정보의 유형 및 규모'(영 제31조의2 제1항 제2호)와 관련하여, 개인정보처리자 중 매출액 규모가 크면서, 개인정보 보유량이 많은 처리자를 우선적으로 고려할 계획이다.

* (고시안) 전년도 연간 매출액이 1,500억원 이상이면서 전년도말 기준 직전 3개월 간 그 정보가 저장·관리되고 있는 정보주체의 수가 일일평균 100만명 이상인 자

- 또한 민감정보나 고유식별정보를 다수 처리하고 있는 개인정보처리자의 경우에도 처리방침 평가 대상으로 고려할 수 있다.

* (고시안) 전년도 말 기준 직전 3개월 간 민감정보 또는 고유식별정보가 저장·관리되고 있는 정보주체의 수가 일일평균 5만명 이상인 자

○ 또한 '개인정보 처리의 법적 근거 및 방식'(영 제31조의2 제1항 제3호)과 관련하여서는 개인정보 보호법 제22조 제3항에 따라 개인정보 처리방침에 명시하도록 한 '개인정보 처리의 법적 근거'가 불명확하거나,

- 개인정보를 자동으로 수집하는 장치의 설치·운영 또는 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템 등) 등 신기술을 활용한 방식으로 개인정보를 처리하는 등의 경우 개인정보 처리방침 평가 대상 선정 시 고려할 수 있다.

○ '법 위반행위 발생 여부'(영 제31조의2 제1항 제4호)와 관련하여서는 개인정보처리자 중 개인정보 유출등 발생 여부와 과징금 및 과태료 처분을 부과받은 적이 있는지 여부를 평가 대상 선정 시 고려한다는 의미이다.

* (고시안) 최근3년 간 법 제34조에 따른 개인정보 유출등이 2회 이상 되었거나, 보호위원회로부터 법 제64조의2에 따른 과징금 또는 법 제75조에 따른 과태료 처분을 받은 자

○ '아동·청소년 등 정보주체의 특성'(영 제31조의2 제1항 제5호)과 관련하여서는 아동이나 청소년을 주요 이용 고객으로 하는 서비스를 운영하는 경우에 평가 대상으로 고려한다는 의미이다.

- 다만, 개인정보처리자가 운영하는 서비스의 이용 고객에 아동이나 청소년이 일부 포함된다고 해서 평가대상으로 선정하는 것은 아니며, 키즈 전용 서비스 등 서비스 제공 목적과 주된 이용 고객 등을 고려할 때 아동이나 청소년을 주요 이용 고객으로 하는 서비스인지 여부를 판단할 계획이다.

○ 향후, 보호위원회에서는 평가 대상 선정을 위한 세부 기준을 「개인정보 처리방침 평가에 관한 고시」 제정을 통해 구체화할 예정이다.

* 본 안내서에서 제시하고 있는 '고시안'은 현재 제정 절차가 진행 중으로, 변경될 수 있음

□ 평가 기준은 개인정보 처리방침에 포함하여야 할 사항을 적정하게 정하고 있는지, 알기 쉽게 작성하였는지, 정보주체가 쉽게 확인할 수 있는 방법으로 공개하고 있는지를 기준으로 하며, 각 기준별 세부 평가지표를 마련하여 객관적으로 평가할 계획이다.

○ 평가 기준에 따른 세부 평가지표는 평가계획 공개 시 함께 공개할 예정이다.

□ 개인정보처리자가 수립하여 공개하고 있는 개인정보 처리방침을 대상으로 평가하며, 평가 과정에서 사실 확인이나 소명 등이 필요한 경우 의견 제출을 요청할 수 있도록 시행령에 평가 절차를 구체화하였다.

○ 보호위원회는 처리방침 평가 내용·일정 등이 포함된 처리방침 평가 계획을 수립하여 평가 개시 10일 전까지 해당 개인정보 처리자에게 통보하고, 평가를 실시할 계획이다.(영 제31조의2 제2항)

○ 보호위원회는 평가 과정에서 필요한 경우 개인정보처리자에게 의견 제출을 요청할 수 있으며, 이에 따라 개인정보처리자가 의견을 제출한 경우 그 내용의 타당성 등을 검토하여 평가에 반영할 수 있다.(영 제31조의2 제3항, 고시안 제5조 제3항)

○ 보호위원회는 처리방침을 평가한 후 그 결과를 지체없이 개인정보처리자에게 통지하여야 하며, 평가를 받은 개인정보처리자는 평가결과에 이의가 있는 경우 평가결과를 통지받은 날로부터 14일 이내에 이의 신청을 할 수 있다.(고시안 제7조 제1항)

○ 보호위원회는 이의신청 내용을 검토하여 그 타당성이 인정되는 경우 평가 결과에 반영하여, 최종적으로 확정된 평가 결과를 대상 개인정보처리자에게 통보한다.(고시안 제7조 제2항)

□ 보호위원회는 개인정보 처리방침 평가를 위해 처리방침 평가위원회를 구성·운영할 수 있다. 평가위원회는 개인정보 처리방침의 적정성, 투명성, 접근성 등을 객관적으로 검토할 수 있도록 다음의 기준에 적합한 20인 이상 50인 이내의 평가 위원을 구성·위촉하며, 평가위원의 임기를 3년으로 연임할 수 있다.

○ 「고등교육법」 제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 6년 이상인 사람

○ 개인정보 보호 관련 업체, 기관 또는 단체(협회, 조합)에서 6년 이상 개인정보 보호 업무에 종사한 사람

○ 그 밖에 개인정보 안전한 활용, 정보보호·보안에 관한 학식과 경험이 풍부한 사람

□ 보호위원회는 개인정보 처리방침 평가 결과 우수한 등급을 받은 개인정보처리자에 대해서는 최대 30%의 범위 내에서 과징금 추가적 감경, 10% 범위 내에서 과태료 감경이 가능하며, 우수사례에 대한 포상 및 홍보 등을 지원할 수 있다.

○ 또한, 처리방침 평가 결과 개선이 필요한 경우 법 제61조 제2항에 따른 개선권고를 할 수 있으며, 법 제66조에 따라 개선권고의 내용 및 결과에 대하여 공표하거나, 개선권고를 받은 자에게 개선권고를 받았다는 사실을 공표할 것을 명할 수 있다.

◈ 「개인정보 처리방침 평가에 관한 고시」(제정안)는 '24년 1월 확정 예정이며, 보다 자세한 사항은 개인정보 처리방침 평가 추진 계획을 수립하여 안내할 예정임(~'24.상반기)

4. 개인정보처리자 유의사항

□ 개인정보처리자는 법 제30조에 따라 개인정보 처리방침에 명시하도록 한 사항을 확인하여 개인정보처리자 스스로의 환경에 맞는 개인정보 처리방침을 마련하여야 한다.

○ 특히 이번 법 개정으로 처리방침에 포함하여야 할 항목에 '법 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우)'과 '법 제28조의2 및 제28조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우)' 등이 추가되었음을 고려하여 개인정보 처리방침을 수립하여야 한다.

< 개인정보 처리방침 포함 사항 >

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
5. 개인정보의 파기절차 및 파기 방법(법 제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
6. 법 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)
7. 개인정보 처리 위탁에 관한 사항(해당되는 경우에만 정한다)
8. 법 제28조의2 및 제28조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)
9. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
10. 법 제31조에 따른 개인정보 보호 책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
11. 법 제31조의2에 따라 국내대리인을 지정하는 경우 국내대리인의 성명, 주소, 전화번호 및 전자우편주소(해당되는 경우에만 정한다)
12. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당되는 경우에만 정한다)
13. 정보주체의 동의 없이 처리할 수 있는 개인정보의 항목과 법적 근거(법 제22조 제3항)
14. 고정형·이동형 영상정보처리기기 운영·관리에 관한 사항(법 제25조 제7항, 제25조의2 제4항)

15. 영 제14조의2 제2항에 따라 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우 같은 조 제1항 각 호의 고려사항에 대한 판단 기준(해당되는 경우에만 정한다)
16. 영 제30조에 따른 개인정보의 안전성 확보 조치에 관한 사항
17. 법 제28조의8 제1항에 따라 정보주체와의 계약의 체결 및 이행을 위하여 개인정보를 국외 처리위탁·보관하는 경우 법 제28조의8 제2항 각 호의 사항(해당되는 경우에만 정한다)
18. 개인정보의 열람청구를 접수·처리하는 부서 <권장>
19. 정보주체의 권익침해에 대한 구제방법 <권장>
20. 개인정보 처리방침 변경에 관한 사항 <권장>

5. 개선 권고 등

개선 권고 요건	개선 권고 등
보호위원회가 개인정보 처리방침 평가 결과 개선이 필요하다고 인정하는 한 경우	법 제61조제2항에 따른 개선 권고 ※ 개선 권고의 내용 및 결과에 대한 공표(법 제66조 제2항), 개선 권고를 받았다는 사실의 공표(법 제66조 제2항) 가능

6. 질의 응답

□ 개인정보 처리방침 평가 대상을 선정하기 위한 세부 기준은?

⇨ 시행령 제31조 제1항 각 호에 따른 사항을 종합적으로 고려하되, 평가 대상 선정을 위한 세부적인 기준은 고시 제정을 통해 구체화 예정

※ 개인정보 보유규모, 개인정보처리자 매출액 등 시행령 제31조의2 제1항의 평가 대상 선정 시 고려사항을 구체화한 일정 기준을 마련할 계획(~'24.1)

⇨ 사업 규모가 큰 개인정보처리자 중 대량의 개인정보를 보유·관리하고 있거나, 민감정보·고유식별정보를 다수 처리하는 개인정보처리자의 처리방침을 우선적으로 평가하되, 그 외 법령 위반 행위 발생 여부, 개인정보 처리의 법적 근거 및 방식 등을 고려하여 평가 대상으로 선정할 계획('24년 50개 내외 평가 예정)

□ 공공기관도 개인정보 처리방침 평가 대상에 포함되는지?

⇨ 공공기관도 개인정보 처리방침 평가 대상 선정 기준에 포함되는 경우 평가 대상이 될 수 있음

⇨ 다만 공공기관은 '24.3월부터 시행되는 개인정보 보호수준 평가를 통해 개인정보 처리방침 작성의 적정성을 포함하여 평가하는 것을 우선으로 하되,

- 개인정보 보호수준 평가 결과 개인정보 처리방침 상의 위험요인이 발견되거나, 기관의 개인정보 보호의 취약점에 대한 사회적 이슈 등이 제기되는 경우 처리방침 평가 대상에 포함하여 평가할 계획

□ 개인정보 처리방침 평가 대상으로 선정되기 위해 신청하는 절차는 없는지?

⇨ 개인정보 처리방침 평가 대상은 평가 대상 선정기준에 해당하는지 여부를 판단하여 보호위원회가 직권으로 선정할 예정으로, 별도의 신청 절차를 두지는 않을 계획임

□ 개인정보 처리방침 평가 시 중점 평가 항목은?

⇨ 법 제30조의2 제1항 각 호의 평가 기준에 따라 평가 예정. 특히 개인정보 처리방침에 명시하여야 할 사항을 적절하게 작성하였는지, 정보주체 관점에서 이해하기 어려운 표현 없이 알기 쉽게 수립되어 있는지 등을 위주로 평가할 계획임. 공정하고 객관적인 평가를 위해 각 평가 기준별 세부 평가지표를 마련하여 평가 전 공개할 예정

□ 개인정보 처리방침 평가 일정은?

⇨ 개인정보 처리방침 평가는 연 1회 또는 2회 추진하는 것으로 계획 중이며, 자세한 일정은 '24년 상반기 중 평가 계획을 수립하여 공개할 예정

□ 개인정보 처리방침 평가 결과에 대해 이의신청 외 별도의 불복 절차는 없는지?

⇨ 개인정보처리자는 개인정보 처리방침 평가 결과를 통보받은 후 평가 결과에 이의가 있는 경우 이의 신청을 할 수 있으며, 보호위원회는 이의 신청 결과까지 종합하여 평가 결과를 확정하여 개선권고 등을 통보함. 다만, 평가 결과가 확정된 이후에는 이에 대한 별도의 불복 절차는 두고 있지 않음

□ 개인정보 처리방침 작성지침은 언제 개정되는지?

⇨ 개인정보 처리방침 작성지침은 개인정보 보호법 개정에 따른 유관 가이드라인 개정과 발맞추어 개정 추진 예정. 2차 시행령 개정 사항까지 종합한 일반형 개인정보 처리방침 작성 지침 개정안을 '24.3월 중 배포 예정임

※ 개인정보 처리방침 작성지침은 개인정보 처리자의 이해를 돕기 위한 예시일 뿐이며, 표준안을 제시하거나 획일적인 처리방침 내용을 유도하는 것이 아님

참고 개인정보 처리방침 평가에 관한 고시(제정안)

* 안내서에서 제시하고 있는 '고시안'은 현재 제정 절차가 진행 중이므로 변경될 수 있음

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다)제30조의2와 같은법 시행령(이하 "영"이라 한다) 제31조의2에 따라 개인정보 처리방침 평가대상 선정과 평가절차 등에 관한 세부기준을 정함을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보 처리방침"(이하 "처리방침"이라 한다)이란 법 제30조에 따라 개인정보 처리 기준 및 보호조치 등에 관해 개인정보처리자가 수립하여 공개한 문서를 말한다.

2. "개인정보 처리방침 평가"(이하 "처리방침 평가"라 한다)란 개인정보보호위원회(이하 "보호위원회"라 한다)가 개인정보처리자의 처리방침이 법 제30조의2제1항 각 호의 기준에 부합하는지 여부를 평가하는 것을 말한다.

3. "평가 대상"이란 보호위원회가 법 제30조의2제1항에 따른 평가를 위하여 영 제31조의2 각 호의 사항을 종합적으로 고려하여 보호위원회가 선정한 처리방침을 말한다.

제3조(평가계획의 수립) ① 보호위원회는 법 제30조의2에 따른 처리방침 평가를 수행하는 경우 평가대상, 기준, 절차 및 일정 등을 정한 평가계획을 수립하여야 한다.

② 보호위원회는 제1항에 따라 평가계획을 수립한 경우 홈페이지 등에 공개할 수 있다.

제4조(평가 대상) ① 영 제31조의2제1항에 따라 평가 대상을 선정하기 위한 세부적 기준은 다음 각 호와 같다.

1. 전년도(법인의 경우에는 전 사업연도를 말한다)의 매출액이 1,500억원 이상이면서 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 정보주체의 수가 일일평균 100만명 이상인 자

2. 전년도 말 기준 직전 3개월 간 법 제23조제1항에 따른 민감정보(이하 "민감정보"라 한다) 또는 법 제24조제1항에 따른 고유식별정보(이하 "고유식별정보"라 한다)가 저장·관리되고 있는 정보주체의 수가 일일평균 5만명 이상인 자(다만, 업무수행을 위해 그에 소속된 임직원의 개인정보를 처리하거나, 다른 공공기관, 법인, 단체의 임직원 또는 개인의 연락처 등 개인정보를 처리한 경우는 제외한다)

3. 처리방침에 법 제22조제3항에 따라 정보주체의 동의 없이 처리할 수 있는 개인정보의 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하지 않은 자

4. 법 제37조의2에 따라 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함한다)으로 개인정보를 처리하거나, 그 밖에 새로운 기술을 이용한 개인정보 처리 방식으로 인하여 정보주체의 개인정보 침해 우려가 있다고 인정되는 자

5. 최근 3년 간 법 제34조에 따른 개인정보 유출등이 2회 이상 되었거나, 보호위원회로부터 법 제64조의2에 따른 과징금 또는 법 제75조에 따른 과태료 처분 등을 받은 자

6. 만14세 미만 아동 또는 만19세 미만 청소년을 주요 이용 대상자로 한 정보통신서비스(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조제2호에 해당하는 서비스를 말한다)를 운영하고 있는 자

② 보호위원회는 필요한 경우 평가 대상을 선정하기 전에 개인정보처리자에게 제1항 각 호의 평가 대상에 해당하는지 여부에 대한 확인을 요청할 수 있다.

제5조(평가 절차) ① 처리방침 평가는 평가계획 수립 및 통지, 평가위원회 구성, 서류 검토 등 평가 수행, 평가 결과 통지 등의 절차에 따라 실시한다.

② 보호위원회는 제4조에 따라 선정된 평가 대상이 법 제30조의2제1항 각 호의 기준에 부합하는지 평가한다.

③ 보호위원회는 영 제31조의2제3항에 따라 개인정보처리자가 의견을 제출한 경우 그 내용의 타당성 등을 검토하여 평가에 반영할 수 있다.

④ 보호위원회는 영 제31조의2제4항에 따라 평가 결과를 지체없이 해당 개인정보처리자에게 통지하여야 한다.

제6조(평가위원회 구성 및 운영) ① 보호위원회는 처리방침 평가를 위해 처리방침 평가위원회(이하 "평가위원회"라 한다)를 구성·운영할 수 있다.

② 평가위원회는 위원장 1명을 포함하여 보호위원회가 위촉하는 20명 이상 50명 이내의 개인정보 보호에 관한 학식과 경험이 풍부한 외부 전문가로 다음 각 호의 경력을 가진 사람 중에서 구성한다.

1. 「고등교육법」 제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 6년 이상인 사람

2. 개인정보 보호 관련 업체, 기관 또는 단체(협회, 조합)에서 6년 이상 개인정보 보호 업무에 종사한 사람

3. 그 밖에 개인정보 안전한 활용, 정보보호·보안에 관한 학식과 경험이 풍부한 사람

③ 평가위원의 임기는 3년으로 하되 연임할 수 있으며, 위원장은 보호위원회 위원장이 위촉한다.

④ 평가위원은 업무에 직접 관여하는 등 직접적인 이해관계가 있거나 공정성을 기할 수 없는 현저한 사유가 있는 경우에는 해당 평가 대상의 평가에 관여할 수 없다.

⑤ 필요한 경우 평가위워원회에 전문위원회를 둘 수 있다.

제7조(이의신청) ① 처리방침 평가를 받은 개인정보처리자는 제5조제4항에 따른 평가결과에 이의가 있는 경우 평가결과를 통보받은 날로부터 14일 이내에 별지 서식을 작성하여 보호위원회에 제출하여야 한다.

② 보호위원회는 제1항에 따른 이의신청을 받은 날로부터 30일 이내에 이의신청 내용을 검토하여 타당성이 인정되는 경우 평가 결과에 반영하여야 하며, 그 결과를 이의신청을 한 자에게 통지하여야 한다. 다만 부득이한 사정이 있는 경우 14일의 범위에서 그 기간을 연장할 수 있다.

제8조(평가결과의 활용 및 지원) ① 보호위원회는 처리방침 평가 결과 개선이 필요한 경우 법 제61조제2항에 따른 개선권고를 할 수 있으며, 법 제66조에 따라 개선권고의 내용 및 결과에 대하여 공표하거나, 개선권고를 받은 자에게 개선권고를 받았다는 사실을 공표할 것을 명할 수 있다. 이 경우 공표 또는 공표명령의 기준은 별표와 같다.

② 제1항에 따라 개선권고를 받은 개인정보처리자는 그 조치결과를 보호위원회에 알려야 하며, 보호위원회는 이행 여부를 점검할 수 있다.

③ 보호위원회는 처리방침 평가 결과 우수한 개인정보처리자에 대하여 포상할 수 있다.

④ 보호위원회는 처리방침 평가 우수 사례를 홍보하거나 컨설팅 지원 등에 활용할 수 있다.

⑤ 보호위원회는 개인정보처리자의 개인정보 처리방침 작성 지침 준수를 위한 지원을 할 수 있다.

제9조(재검토기한) 보호위원회는 이 고시에 대하여 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2023년 11월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 10월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

※ 별표 및 별지 서식은 개인정보위 홈페이지(www.pipc.go.kr) 공지사항의 행정예고안 참조

2 영상정보처리기기 규정 개정

1 고정형 영상정보처리기기(법 제25조)

1. 개정 개요

□ 최근 기술발전 추세를 고려하여 공개된 장소에서 고정형 영상정보처리기기(예 : CCTV)를 설치·운영할 수 있는 경우를 일부 확대하였으며,

○ 범죄·화재 예방, 교통단속 등의 목적 외에도 인구밀집도 분석, 디지털 광고 등에 활용 가능(영상을 저장하지 않는 경우에 한함)하도록 개정하였다.

□ 아울러, 고정형 영상정보처리기기는 정당한 권한 있는 자에 한하여 설치·운영 가능하다는 점을 명확히 하는 등 그동안의 제도 운영상 미비점을 보완하여,

○ 시설안전 및 관리, 화재예방, 교통단속, 교통정보 수집·분석 등을 목적으로 하는 CCTV는 정당한 권한 없이 임의로 설치·운영할 수 없도록 명확하게 하였다.

2. 법령

법률	**제25조(고정형 영상정보처리기기의 설치·운영 제한)** ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치·운영하여서는 아니 된다. 1. 법령에서 구체적으로 허용하고 있는 경우 2. 범죄의 예방 및 수사를 위하여 필요한 경우 3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우 4. 교통단속을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우 5. 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우 6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우 ② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다. ③ ~ ⑤ (생략) ⑥ 고정형영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다. ⑦ ~ ⑧ (생략)

시행령	**제22조(고정형 영상정보처리기기 설치·운영 제한의 예외)** ① 법 제25조제1항제6호에서 "대통령령으로 정하는 경우"란 다음 각 호의 어느 하나에 해당하는 경우를 말한다. 1. 출입자 수, 성별, 연령대 등 통계값 또는 통계적 특성값 산출을 위해 촬영된 영상정보를 일시적으로 처리하는 경우 2. 그 밖에 제1호에 준하는 경우로서 보호위원회의 심의·의결을 거친 경우 ② ~ ③ (생략)

3. 개정내용 해설

□ 도로, 공원 등 불특정 다수가 이용하는 공개된 장소에서 고정형 영상정보처리기기(CCTV)를 설치·운영할 수 있는 경우를 확대하였는데,

○ 주차장 요금징수 등에 CCTV가 널리 활용되고 있음을 반영하여 CCTV 설치·운영 가능 사유에 '시설 관리' 목적(제25조제1항제3호)을 추가하였고,

○ 인구밀집도 분석, 디지털 광고 등을 위해 촬영한 영상을 저장하지 않고 통계값 또는 특성값을 산출하는 용도로만 활용하는 경우(제25조제1항제6호)를 허용하였다.

* (예시) 출입자 수, 성별, 연령대 등 통계값 또는 통계적 특성값 산출을 위해 촬영된 영상정보를 저장하지 아니하고 일시적으로 처리하는 경우

4. 개인정보처리자 유의사항

□ 시설안전 및 관리, 화재예방, 교통단속, 교통정보 수집·분석 등을 목적으로 하는 CCTV는 정당한 권한을 가진 자에 한하여 설치·운영할 수 있다고 규정되어 있는데,

○ 이는 촬영 장소에 대한 정당한 권한 없이 임의로 CCTV를 설치하여 공개된 장소를 촬영하는 행위를 원칙적으로 제한한다는 점을 명확히 한 것이다.

< 관련 사례 >

▸ 교통단속 권한이 없는 아파트 관리사무소가 진입로 도로상에 CCTV를 설치하여 불법 유턴이나 신호위반을 단속하는 경우는 정당한 권한 없는 CCTV 설치에 해당

▸ 시설안전이나 화재예방을 이유로 다른 사람의 소유지나 사업소 내부를 비추는 CCTV를 설치하여 영상을 촬영하는 행위는 정당한 권한 없는 CCTV 운영에 해당

□ 또한, 이번에 신설된 제25조제1항제6호는 촬영된 영상정보를 저장하지 아니하는 것을 전제로 하여 통계값 또는 통계적 특성값 산출을 위한 목적의 고정형 영상정보처리기기 설치·운영을 허용하는 내용이므로, 이와는 달리 촬영된 영상을 일정기간 동안 저장하고 있는 고정형 영상정보처리기기와는 구분되어야 한다.

○ 따라서, 같은 항 제1호부터 제5호에 따른 목적(예 : 범죄예방, 시설안전 등)으로 설치·운영하는 고정형 영상정보처리기기는 촬영한 영상정보를 저장해야 하므로 그 영상정보를 통계작성, 과학적 연구, 공익적 기록보존 목적으로 이용하고자 하는 경우에는 법 제28조의2에 따라 해당 영상정보를 가명처리한 후 이용하여야 한다.

< 관련 사례 >

▸ 사업장내 범죄예방, 시설안전 등을 목적으로 다수 설치.운영 중인 CCTV 영상을 일정기간 저장함과 동시에 촬영된 영상을 활용하여 시설 이용자 수, 성별, 연령대 등의 통계값 또는 통계적 특성값을 도출하려는 경우에는 먼저 특정 개인을 알아볼 수 없도록 가명처리한 후 활용 가능

5. 제재 규정

위반행위	제재 내용
제25조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기를 설치·운영한 자	3천만원 이하 과태료 (제75조제2항제10호)
제25조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기를 설치·운영한 자	5천만원 이하 과태료 (제75조제1항제1호)
제25조제5항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자	3년 이하의 징역 또는 3천만원 이하의 벌금(제72조제1호)
제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)을 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자	3천만원 이하 과태료 (제75조제2항제5호)

6. 질의 응답

□ 영상정보처리기기가 고정형 및 이동형으로 세분화되었는데, 이에 따라 안내판 표기도 변경해야 하는지?

⇨ 원칙적으로는 영상정보처리기기의 안내판 설치 시, 법정 용어인 '이동형' 및 '고정형'을 사용하시는 것을 권고드림. 다만, 사회 통념상 CCTV는 고정형 영상정보처리기기를 의미하므로 기존 안내판에 "CCTV"로 표기된 명칭을 "고정형 CCTV" 또는 "고정형 영상정보처리기기"로 굳이 변경하지 않아도 무방함

□ 24시간 동안 특정한 조건(예:모션감지) 하에 촬영이 이루어지는 경우에도 CCTV 안내판에 촬영 시간을 24시간으로 고지하는 것이 가능한지?

⇨ "고정형 영상정보처리기기"란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하는 장치를 말함. 따라서, CCTV를 24시간 동안 운영하면서 연속적으로 촬영이 이루어지는 방식이나 특정한 조건 하에 촬영이 이루어지는 방식 모두 해당 장소를 통행하는 사람에 대한 촬영이 발생하는 결과를 초래한다고 볼 수 있으므로, "촬영시간"을 24시간으로 고지 가능

□ 주차장 요금 징수 및 이용자 안전을 위한 CCTV 설치·운영이 가능한지?

⇨ 보호법 제25조제1항제3호에 따라 '시설의 안전 및 관리'를 목적으로 CCTV를 설치·운영할 수 있으며, '시설의 안전 및 관리'에는 해당 시설을 이용하는 이용자의 안전과 주차장 이용 요금징수 등과 같은 해당 시설의 정상적인 운영을 위해 필요한 경우도 포함될 수 있음

다만, 동 조항은 해당 시설의 소유자 또는 관리자 등과 같은 정당한 권한을 가진 자에 한하여 적용될 수 있으므로 그러한 권한이 없는 자에 의한 CCTV 설치·운영은 제한됨

□ 매장 내 방문객 수 집계를 목적으로 CCTV 설치·운영이 가능한지?

⇨ 불특정 다수가 출입이 가능한 공개된 매장 내에서, 촬영된 영상을 저장하지 아니하면서 방문객 수 집계 등의 통계값이나 예상 성별, 연령대 등 통계적 특성값 산출을 목적으로 촬영된 영상을 일시적으로 처리하는 경우라면 보호법 제25조제1항제6호에 해당될 수 있으므로 해당 목적의 CCTV의 설치·운영 가능

다만, 범죄예방이나 시설안전 등을 목적으로 기 설치.운영 중에 있는 CCTV 영상을 저장하면서 위에 언급된 통계값이나 통계적 특성값을 산출하려고 하는 경우에는 보호법 제25조제1항제6호에 해당하지 아니하므로 같은 법 제28조의2에 따라 특정 개인을 알아볼 수 없도록 가명처리한 후 통계작성, 과학적 연구 등의 목적으로 활용하여야 함

② 이동형 영상정보처리기기(법 제25조의2)

1. 개정 개요

□ 공개된 장소 등에서 업무 목적으로 이동형 영상정보처리기기를 이용하여 개인영상정보를 촬영하는 행위를 원칙적으로 제한하되,

○ 개인정보 수집·이용 사유(제15조제1항 각 호*)에 해당하거나, 정보주체가 촬영 사실을 알 수 있었으나 거부의사를 밝히지 않은 경우 촬영할 수 있도록 하였다.

* 정보주체의 동의를 받은 경우, 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우 등

□ 촬영을 하는 경우에는 불빛, 소리, 안내판 등으로 촬영 사실을 표시하도록 하는 등 이동형 영상정보처리기기의 운영 기준을 마련하여,

○ 자율주행차, 로봇, 드론 등이 주행 경로 주변의 영상을 촬영하여 장애물 파악 및 회피 등에 활용할 수 있도록 하였다.

2. 법령

법률	**제2조(정의)** 이 법에서 사용하는 용어의 뜻은 다음과 같다. 1. ~ 7. (생략) 7의2. "이동형 영상정보처리기기"란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다. **제25조의2(이동형 영상정보처리기기의 운영 제한)** ① 업무를 목적으로 이동형 영상정보처리기기를 운영하려는 자는 다음 각 호의 경우를 제외하고는 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상(개인정보에 해당하는 경우로 한정한다. 이하 같다)을 촬영하여서는 아니 된다. 1. 제15조제1항 각 호의 어느 하나에 해당하는 경우 2. 촬영 사실을 명확히 표시하여 정보주체가 촬영 사실을 알 수 있도록 하였음에도 불구하고 촬영 거부 의사를 밝히지 아니한 경우. 이 경우 정보주체의 권리를 부당하게 침해할 우려가 없고 합리적인 범위를 초과하지 아니하는 경우로 한정한다. 3. 그 밖에 제1호 및 제2호에 준하는 경우로서 대통령령으로 정하는 경우 ② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있는 곳에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하여서는 아니 된다. 다만, 인명의 구조·구급 등을 위하여 필요한 경우로서 대통령령으로 정하는 경우에는 그러하지 아니하다. ③ 제1항 각 호에 해당하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판 등 대통령령으로 정하는 바에 따라 촬영 사실을 표시하고 알려야 한다.

	④ 제1항부터 제3항까지에서 규정한 사항 외에 이동형 영상정보처리기기의 운영에 관하여는 제25조제6항부터 제8항까지의 규정을 준용한다.
시행령	**제3조(영상정보처리기기의 범위)** ① (생략) ② 법 제2조제7호의2에서 "대통령령으로 정하는 장치"란 다음 각 호의 장치를 말한다. 1. 착용형 장치: 안경 또는 시계 등 사람의 신체 또는 의복에 착용하여 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치 2. 휴대형 장치: 이동통신단말장치 또는 디지털 카메라 등 사람이 휴대하면서 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치 3. 부착·거치형 장치: 차량이나 드론 등 이동 가능한 물체에 부착 또는 거치(据置)하여 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치 **제27조(이동형 영상정보처리기기 운영 제한의 예외)** 법 제25조의2제2항 단서에서 "대통령령으로 정하는 경우"란 범죄, 화재, 재난 또는 이에 준하는 상황에서 인명의 구조·구급 등을 위하여 사람 또는 그 사람과 관련된 사물의 영상(개인정보에 해당하는 경우로 한정한다. 이하 같다)의 촬영이 필요한 경우를 말한다. **제27조의2(이동형 영상정보처리기기 촬영 사실 표시 등)** 법 제25조의2제1항 각 호에 해당하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판, 안내서면, 안내방송 또는 그 밖에 이에 준하는 수단이나 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 한다. 다만, 드론을 이용한 항공촬영 등 촬영 방법의 특성으로 인해 정보주체에게 촬영 사실을 알리기 어려운 경우에는 보호위원회가 구축하는 인터넷 사이트에 공지하는 방법으로 알릴 수 있다.

3. 개정내용 해설

□ 신설된 법 제25조의2 규정은 불특정 다수가 이용하는 공개된 장소에서 이동형 영상정보처리기기를 통해 개인정보에 해당하는 영상을 촬영하는 경우에 적용되며,

○ 원칙적으로 업무 목적이 아닌 사적인 용도(예 : 자동차 블랙박스*, 취미활동 등)로 이동형 영상정보처리기기를 통해 영상을 촬영하는 경우에는 적용되지 않는다.

* 일반적으로 자동차 블랙박스는 교통사고 발생시 증거확보를 목적으로 하고 있고, 자동차의 종류와 관계없이 교통사고는 예상치 못하게 우연히 발생하는 일에 해당하므로 업무 목적에 해당하지 않음
다만 촬영된 영상을 저장하여 별도의 업무상 목적으로 활용하는 경우에는 보호법 적용 대상에 해당

○ 다만, 목욕실, 화장실, 탈의실 등과 같이 개인의 사생활을 현저히 침해할 우려가 있는 장소에서 이동형 영상정보처리기기로 개인정보에 해당하는 영상을 촬영하는 행위는 업무 목적이나 사적인 용도 여부와 관계없이 엄격히 제한된다.

□ 동 신설 규정에 따라 자율주행차, 배달로봇, 드론 등의 유·무인 이동체가 촬영 사실을 명확히 표시하여 정보주체가 알 수 있도록 한 경우에는 주행 경로상의 영상을 촬영하여 장애물 파악 및 회피 등을 위해 활용할 수 있다.

○ 다만, 정보주체가 촬영 거부의사를 명확히 밝힌 경우에는 촬영을 할 수 없는데, 고속 주행 등으로 거부의사 파악이 어렵거나 수용하기 어려운 상황이 예상되는 경우에는 주행이 완료된 후 사건사고 발생 등으로 추가적 확인이 필요한 영상을 제외하고는 지체없이 삭제하거나 개인을 알아볼 수 없도록 가명처리하도록 설정하여 정보주체의 권리가 침해될 가능성을 사전에 예방하는 것이 바람직하다.

* 보호법 제35조~제38조에 따라 정보주체는 자신의 개인정보를 처리하는 개인정보처리자에게 처리정지, 삭제 등을 요구할 수 있으며, '23.12월 현재 자율주행차가 상용화되지 않은 상황을 고려할 때 연구용 자율주행차 운행 사업자, 배달로봇 또는 드론 서비스 사업자가 개인정보처리자에 해당될 수 있음

□ 또한, 이동형 영상정보처리기기를 통해 업무상 목적으로 촬영한 개인 영상의 안전성 확보 조치, 운영·관리 방침 마련, 공공기관 업무위탁 절차 및 요건 등에 관하여는 법 제25조의2제4항에 따라 고정형 영상정보처리기기와 동일하게 준용된다.

4. 개인정보처리자 유의사항

□ 이동형 영상정보처리기기의 촬영사실 표시는 불빛, 소리, 안내판 등 법령에 규정된 몇 가지 방법으로만 제한되는 것이 아니며, 해당 영상기기의 고유한 특성과 촬영을 하는 상황에 따라 가용한 방법 및 수단 등을 종합적으로 고려하여 하나 이상의 방법(Multi-channel)을 통해 정보주체가 촬영사실을 알 수 있도록 표시하여야 한다.

※ (예시) 영상 촬영에 관한 표지판이나 안내지(입장권, 포스터 등)에 게제, 영상기기 표면에 안내문구가 기재된 스티커 부착, LED 또는 섬광등 불빛 표시, 영상기기 조작자를 쉽게 알 수 있는 옷차림(형광색 옷 등), 피촬영자 직접 고지, 무선 신호, QR코드, SNS 또는 홈페이지를 통한 공지 등

○ 다만, 과도한 불빛이나 너무 큰 소리를 통해 촬영사실을 표시하는 것은 일상의 평온함을 해칠 우려가 크고, 교통사고 등의 위험도 증가할 수 있기 때문에 가급적 문자나 그림(QR 코드 포함), LED 불빛 등을 통해 촬영사실을 표시하는 방안을 고려하는 것이 바람직하다.

□ 드론을 이용한 항공촬영*의 경우에는 촬영방법의 특성으로 인해 불빛이나 소리 등을 통해서도 정보주체에게 촬영사실을 알리는 것이 매우 어려운 점이 있다.

* 개인적 용도(취미 등)의 드론 촬영은 해당하지 않으며 업무상 목적의 드론 촬영에 한함

○ 따라서, 업무를 목적으로 드론을 이용하여 불특정 다수가 촬영될 수 있는 지역을 촬영하는 경우에는 개인정보위가 구축·운영하는 인터넷 사이트(www.privacy.go.kr ▸기업·공공서비스 ▸드론 촬영사실 공지)를 통해 촬영목적과 범위, 관리책임자 연락처 등을 공지하는 것이 필요하다.

□ 아울러, 바디캠을 이용한 촬영의 경우에는 촬영자와 피촬영자가 매우 근접한 상황에서 촬영이 이루어지기 때문에 개인 식별성이 매우 높은 영상이 촬영되고 상호간의 대화 내용까지 녹음될 수 있는 특성이 있다.

○ 따라서, 바디캠을 업무상 목적으로 활용하려는 경우에는 촬영 사실과 목적 등을 피촬영자에게 직접적으로 명확히 고지하여 피촬영자의 승낙 하에 촬영이 이루어지도록 하는 것이 바람직하다.

□ 개인정보위에서 권고하는 주요 이동형 영상정보처리기기별 촬영사실 표시 방법은 아래와 같으며, 앞으로도 기술 발전 추세 등을 고려하여 관련 전문가 및 산업계와의 긴밀한 소통을 통해 기기 유형별로 표준화된 촬영사실 표시 방법을 지속 보완하고 그림문자, 안내문구 등을 표준화할 예정이다.

구분	촬영사실 표시 방법	필수 표시내용
자율주행차*	▸ 기기 외관에 문자 표시 부착 (스티커 또는 데칼) ▸ QR코드, LED 불빛 등 병행 가능	▸ 촬영된다는 사실 ▸ 촬영 주체 ▸ 관리책임자 연락처, 촬영 목적 및 범위 등(처리방침에 포함하여 인터넷 홈페이지 공지 가능)
로봇	▸ 기기 외관에 문자 표시 부착 및 주요 거점 안내판 부착(X배너 등) ▸ 운영상황에 따라 LED 불빛이나 안내소리 등 추가	〃
드론	▸ 개인정보위 홈페이지 공지 및 주요 거점 안내판 부착(X배너 등) ▸ 야간 촬영시 LED불빛 추가 ▸ 운영상황에 따라 행사장 입장권 또는 포스터 표기, 드론 조작자의 형광색 옷차림 등 추가	▸ 촬영 주체, 목적, 지역, 기간, 관리책임자 연락처(서면, 안내판, 개인정보위 홈페이지를 통한 공지 가능)
바디캠	▸ 피촬영자에게 직접 고지하거나 촬영사실을 알 수 있는 옷차림 착용 ▸ 촬영시 LED 불빛 표시 병행	▸ 촬영된다는 사실 ▸ 촬영 주체 ▸ 관리책임자 연락처, 촬영 목적 및 범위 등(처리방침에 포함하여 인터넷 홈페이지 공지 가능)

* '23.12월말 기준 상용화 전 단계임을 고려할 때 연구용 시범운행 자율주행차를 대상으로 함

○ 촬영사실 표시 의무는 사업자 입장에서는 영상 촬영시 발생할 수 있는 민원이나 사생활 침해 논란 등을 사전에 예방할 수 있고, 정보주체 입장에서는 누가 어떠한 목적으로 영상을 촬영하는지 알 수 있기 때문에 실질적 권리행사가 가능해지는 장점이 있다.

□ 이번에 신설된 법 제25조의2제1항제2호는 정보주체의 권리 보장(촬영사실 명확히 표시, 거부의사 없는 경우, 부당한 권리침해 및 합리적 범위 초과 금지 등)을 전제로 하여 이동형 영상정보처리기기를 통한 업무상 촬영을 허용하는 내용이다.

○ 따라서, 조사, 단속 등의 업무와 같이 본질적으로 정보주체의 권리행사(처리정지, 삭제 요구 등)를 수용할 수 없는 성격의 업무에 대하여는 동 조항이 적용되지 않으며, 그러한 업무를 수행하기 위한 영상 촬영은 같은 항 제2호에 따라 법 제15조제1항 각 호의 어느 하나*에 따른 법적 근거를 갖추어야 한다.

* (예시) 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 등

□ 공개된 장소에서 촬영된 불특정 다수의 영상을 별도로 저장하여 AI 학습 등 업무상 목적으로 활용하는 것은 피촬영자가 그 내용을 예측할 수 없다는 측면에서 부당한 권리침해 우려가 있으므로 특정 개인을 알아볼 수 없도록 익명·가명처리가 필요하다.

○ 다만, 개인정보위는 보행자 안전 확보 등을 위한 기술개발시 익명·가명처리된 영상을 통해서는 기술경쟁력 확보가 어려운 점을 고려하여 개인 식별 목적이 아닌 연구개발 분야에 한하여 규제샌드박스 실증특례 제도를 통해 엄격한 안전조치 이행을 조건으로 영상데이터 원본 활용을 제한적으로 허용*할 예정이다.

* '23.11.14. 개인정보위 보도자료 참조(신산업 성장 촉진을 위한 데이터경제 활성화 핵심과제 추진)

< 관련 사례 >

▸ '부당한 권리침해 우려'에 대한 판단은 보호법상 일반원칙(§3, §15 등)에 비추어 사회통념상 피촬영자가 예측 가능한 수준에서 이용 가능 범위 검토 필요

√ **(사건·사고 발생 시)** 급박한 생명·신체·재산의 이익을 위하여 필요한 경우에 해당

√ **(장애물회피, 물품배송, 시설안전)** 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체 권리보다 우선하는 경우에 해당. 단 안전조치 필요

▸ 다만, 부당한 권리침해 발생 여부는 구체적·개별적 사안에 따라 판단할 사항으로, 향후 판단기준 구체화 및 유형별 사례 제시

◈ 이동형 영상정보처리기기에 대한 별도 안내서를 발간할 예정(~'24.상반기)이며, 수집한 영상정보에 대한 활용 등 개별적으로 궁금한 사안이 있는 경우 개인정보위에서 운영 중인 '사전 적정성 검토', '민원상담' 등을 통해 계속하여 안내해 나갈 계획임

5. 제재 규정

위반행위	제재 내용
제25조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 자	3천만원 이하 과태료 (제75조제2항제11호)
제25조의2제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 자	5천만원 이하 과태료 (제75조제1항제2호)
제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)을 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자	3천만원 이하 과태료 (제75조제2항제5호)

6. 질의 응답

□ 업무를 목적으로 이동형 영상기기 운영 시, 촬영 사실의 명확한 표시 및 정보주체의 동의가 모두 필요한지?

⇨ 업무를 목적으로 한 촬영이라는 사실을 명확히 표시하여 정보주체가 촬영사실을 알 수 있도록 하였음에도 불구하고 정보주체가 촬영 거부 의사를 밝히지 아니한 경우에 해당하고, 정보주체의 부당한 권리 침해 우려가 없으며 합리적 범위를 초과하지 않는다면, 정보주체의 별도 동의는 필요하지 않음

□ 드론을 이용한 항공촬영 시에는 불빛, 소리, 안내판 등을 통해서도 촬영사실을 알리기 어려운 특성이 있는데?

⇨ 드론에 의한 항공촬영 등 촬영 방법의 특성으로 인해 정보주체에게 촬영 사실을 알리기 어려운 경우에는 보호위원회가 구축하는 인터넷 사이트를 통해 공지하는 방법으로 알릴 수 있음
해당 인터넷 사이트는 개인정보포털(www.privacy.go.kr ▸기업·공공서비스 ▸ 드론 촬영 사실 공지)을 말하며, 향후 '24년부터는 국토부, 국방부의 드론 비행 및 촬영승인 절차와 연계하여 일괄 처리하는 방안 검토 중

□ 정보주체의 촬영거부 의사표현 방식은 어떤 것이 있는지?

⇨ 정보주체가 영상 촬영을 거부하는 의사표현 방식에 대해서는 별도의 제한을 두고 있지 않으므로 사회 통념상 자신의 의사를 다른 사람에게 명확히 알릴 수 있는 모든 형태의 표현 방식(문자, 음성, 행동 등)이 포함될 수 있음

□ 유튜버 등 영상크리에이터가 거리를 지나는 불특정 다수 행인들의 영상을 마음대로 촬영하여 인터넷에 공개하는 경우 보호법을 적용할 수 있는지?

⇨ 유튜버 등의 경우에도 업무 목적이 인정되는지 여부에 따라 보호법 적용 가능함
국세청은 유튜버, BJ 등 신종 직업군에 대한 과세기준을 마련하여 시행하고 있으며, 영상 콘텐츠를 지속 생산하면서 수익이 발생하는 경우 사업자등록이 필수 사항임
또한 수익 목적인 경우에는 광고물 부착을 위한 별도의 상업용 계정을 발급받아야 함

□ 시행령에서 이동형 영상정보처리기기 관련하여 정보주체에게 촬영사실을 안내하게 되어있는데, 개인 차량이나 화물차의 블랙박스의 경우에는 어떻게 해야 하는지?

⇨ 자동차 블랙박스는 일반적으로 교통사고 발생시 원인을 파악하고 대응하기 위한 목적으로 설치·운영되고 있으며, 교통사고는 운전자의 본질적인 업무 목적으로 보기 어렵기 때문에 불빛, 소리, 안내판 등을 통해 촬영사실을 표시할 필요는 없음
다만, 촬영된 영상을 저장하여 별도의 업무 목적(예 : 주행기술 개발, 지도제작 등)으로 활용하는 경우에는 촬영사실을 표시해야 하며, 자동차의 경우는 차량 외부에 LED를 설치하거나 스티커를 부착하여 촬영사실을 표시하고 알리는 것이 바람직

□ 이동형 영상정보처리기기에 대해서도 운영관리 방침을 마련하여 공개해야 하는지?

⇨ 업무를 목적으로 공개된 장소를 촬영하는 이동형 영상정보처리기기는 운영관리 방침을 마련하여 공개하여야 하며 운영관리 방침에 포함되어야 할 내용 등 구체적인 사항은 「표준개인정보보호지침」(개인정보위 고시)에 반영하여 공개할 예정임
아울러, '이동형 영상정보처리기기 운영관리 방침'에 포함하여야 할 사항을 '개인정보처리방침' 또는 '고정형 영상기기 운영관리 방침'에 포함하여 공개한 경우에는 별도로 방침을 마련하여 공개할 필요는 없음

□ 이동형 영상정보처리기기도 녹음 기능 사용 가능한지?

⇨ 원칙적으로 보호법 제25조의2 에서는 이동형 영상기기를 통한 영상 촬영에 관하여 규정하고 있으므로, 음성 녹음에 대해서는 제15조의 일반원칙이 적용됨
따라서, 녹음된 내용이 특정 개인을 알아볼 수 있는 개인정보에 해당하는 경우에는 정보주체 동의 등의 법적 근거를 갖추어야 함. 아울러 공개되지 아니한 타인간의 대화 녹음시에는 통신비밀보호법 위반에도 해당될 수 있음을 유의할 필요

□ 영상이 촬영되었는지 여부가 불분명한 사람이 자신의 영상에 대한 열람이나 삭제를 요청하는 경우 어떻게 대응해야 하는지?

⇨ 정보주체는 자신의 개인정보에 대한 결정권을 가지므로, 원칙적으로 특정 영상에 포함된 정보주체가 자신의 영상에 대한 열람, 삭제 등을 요구하는 경우에는 정당한 사유없이 이를 제한하거나 거절할 수 없음

다만, 개인정보보호법 상의 권리행사 요구는 정보주체 본인 영상에 한하므로 그러한 요구가 있는 경우 해당 정보주체가 촬영된 영상인지, 다른 사람의 권리를 침해할 우려가 있는지를 명확하게 확인해야 함

□ 「민원처리에 관한 법률」 제4조에 따라 민원인 등의 폭언, 폭행 등 발생시 민원처리 담당자를 보호하기 위해 휴대용 영상음성기록장비 사용이 가능한데, 동 법률 조항과 보호법 제25조의2 규정 중 어느 법률이 우선 적용되는지?

⇨ 보호법 제25조의2 제1항 제1호에 따라 동 법률 제15조제1항 각 호의 어느 하나에 해당하는 경우(법률에 특별한 규정이 있는 경우 등)에는 이동형 영상정보처리기기를 통해 개인영상을 촬영할 수 있음. 또한 보호법 제6조에 따라 다른 법률에 특별한 규정이 있는 경우에는 해당 법률 규정을 우선 적용하는 것이 원칙이므로 「민원처리에 관한 법률」에서 특별히 정하는 사항은 해당 법률이 우선 적용됨

3 수집 출처 및 이용·제공 내역 통지 제도

1 개인정보 수집 출처 등 통지(법 제20조, 영 제15조의2)

1. 개정 개요

□ 정보통신서비스 특례규정(제39조의8) 삭제로 개인정보 이용·제공내역 통지제도(제20조의2 신설)가 일반 개인정보처리자로 확대됨에 따라,

○ 기존 '수집출처 통지'제도와 '이용·제공내역 통지'제도가 실효성 있게 연계되어 합리적인 통지 제도로 자리 잡을 수 있도록 개선하였다.

2. 법령

법률	**제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 통지)** ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다. 1. 개인정보의 수집 출처 2. 개인정보의 처리 목적 3. 제37조에 따른 개인정보 처리의 정지를 요구하거나 동의를 철회할 권리가 있다는 사실
시행령	**제15조의2(개인정보 수집 출처 등 통지 대상·방법·절차)** ① 법 제20조제2항 본문에서 "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다. 이 경우 다음 각 호에 규정된 정보주체의 수는 전년도 말 기준 직전 3개월 간 일일평균을 기준으로 산정한다. 1. 5만명 이상의 정보주체에 관하여 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 법 제24조제1항에 따른 고유식별정보(이하 "고유식별정보"라 한다)를 처리하는 자 2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자 ② 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 법 제20조제1항 각 호의 사항을 다음 각 호의 어느 하나에 해당하는 방법으로 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알려야 한다. 다만, 법 제17조제2항제1호부터 제4호까지의 사항에 대하여 같은 조 제1항제1호에 따라 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 기산하여 연 1회 이상 정보주체에게 알려야 한다. 1. 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법 2. 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법 ③ 개인정보처리자는 법 제20조제2항에 따라 개인정보의 수집 출처 등에 관한 사항을 알리는 것과 법 제20조의2제1항에 따른 이용·제공 내역의 통지를 함께 할 수 있다.

	④ 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 제2항에 따라 알린 경우 다음 각 호의 사항을 법 제21조 또는 제37조제5항에 따라 해당 개인정보를 파기할 때까지 보관·관리하여야 한다. 1. 정보주체에게 알린 사실 2. 알린 시기 3. 알린 방법

3. 개정내용 해설

□ 법 제20조의 정보주체 이외로부터 수집한 개인정보의 수집 출처 등의 통지는 정보주체의 요구가 있는 경우에 하는 기존 제도는 종전 내용을 유지하였으나,

○ 법 제20조제2항에서 정하는 의무적으로 수집 출처 등의 통지를 해야 하는 대상을 정할 때의 정보주체의 수 산정기준을 법 제20조의2에 따른 이용·제공 내역 통지의 산정기준과 동일하게 정비하였다.(전년도 말 기준 직전 3개월 간 일일평균)

□ 또한, 법 제20조제2항에 따라 의무적으로 수집 출처 등에 관한 사항을 알리는 것과 법 제20조의2제1항에 따른 이용·제공 내역의 통지를 함께 할 수 있도록 하였으며,

○ 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법* 외에도 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법을 추가하여 통지 방법을 다양화하였다.

* 팩스의 경우는 불특정 다수에게 노출될 수 있는 방법인 점을 고려하여 제외함

4. 개인정보처리자 유의사항

□ 수집 출처 등의 통지를 의무적으로 해야 하는 의무대상을 판단하기 위한 정보주체의 수 산정기준(영 제15조의2제1항 후단)과 관련된 개정규정에 대하여는 2024년 1월 1일부터 시행하도록 하였다. (영 부칙 제1조제2호)

○ 정보주체의 수 산정은 전년도 10월 1일부터 12월 31일까지 매일 저장·관리되고 있는 정보주체 수의 총합을 92(일)로 나눈 수가 100만명 이상인 경우(민감정보·고유식별정보의 경우 5만명 이상)를 의미한다.

5. 제재 규정

위반행위	제재 내용
정보주체에게 수집 출처 등의 사실을 알리지 아니한 자 (제20조제1항・제2항 위반)	3천만원 이하의 과태료 (제75조제2항제2호)

6. 질의 응답

□ 수집 출처 통지와 이용·제공 내역 통지의 대상자 판단 기준이 동일한데, 시행령 제15조의2 단서 조항(전년도 말 기준 직전 3개월간 일일평균을 기준)의 시행 일자가 2024년 1월 1일인데, 시행령 제15조의3에는 경과조치가 없는 이유는?

⇨ 부칙에서 수집 출처 통지의 단서 조항만 시행 일자를 지정한 이유는 수집 출처 통지의 경우 대상을 산정하는 기준의 시점이 이번 개정으로 새로 도입되는 것이므로 부칙에서 기준일자를 정한 것이며, 기존 이용·제공 내역 통지 제도의 경우 이전 시행령 제48조의6에 동일한 기준이 있으므로 개정법 시행에도 변동사항이 없으므로 별도 경과조치를 정하지 않은 것임

□ 수집 출처 통지 시 시행령 제15조의2제2항에 따라 3개월 이내에 정보주체에게 알려야 하는데, 3개월이 지난 후에 제3항에 따라 이용·제공 내역과 함께 통지해도 되는지?

※ 예) 1월에 개인정보를 제공받았는데, 3개월 이내에 별도 통지하지 않고 10월에 발송하는 이용·제공 내역 통지에 포함하여 발송하는 경우

⇨ 3개월 이내에 정보주체에게 알리는 것이 원칙이며, 해당 기간 내에 이용·제공 내역 통지 시 함께 통지할 수 있음

② 개인정보 이용 · 제공내역의 통지(법 제20조의2, 영 제15조의3)

1. 개정 개요

□ 정보통신서비스 제공자 특례규정(제39조의8)에만 있던 개인정보 이용·제공 내역의 통지 제도를 모든 개인정보처리자를 대상으로 하는 일반규정으로 확대하였으며,

○ 이용·제공 내역의 통지 대상의 기준 및 제외 사유를 시행령에 명확히 규정하였다.

□ 또한, 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 알림창 등을 통해 알릴 수 있도록 하여 통지 방법을 다양화하였다.

2. 법령

법률	**제20조의2(개인정보 이용·제공 내역의 통지)** ① 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 이 법에 따라 수집한 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 주기적으로 정보주체에게 통지하여야 한다. 다만, 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집·보유하지 아니한 경우에는 통지하지 아니할 수 있다. ② 제1항에 따른 통지의 대상이 되는 정보주체의 범위, 통지 대상 정보, 통지 주기 및 방법 등에 필요한 사항은 대통령령으로 정한다.
시행령	**제15조의3(개인정보 이용·제공 내역의 통지)** ① 법 제20조의2제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다. 이 경우 다음 각 호에 규정된 정보주체의 수는 전년도 말 기준 직전 3개월 간 일일평균을 기준으로 산정한다. 1. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자 2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자 ② 법 제20조의2제1항에 따른 통지의 대상이 되는 정보주체는 다음 각 호의 정보주체를 제외한 정보주체로 한다. 1. 통지에 대한 거부의사를 표시한 정보주체 2. 개인정보처리자가 업무수행을 위해 그에 소속된 임직원의 개인정보를 처리한 경우 해당 정보주체 3. 개인정보처리자가 업무수행을 위해 다른 공공기관, 법인, 단체의 임직원 또는 개인의 연락처 등의 개인정보를 처리한 경우 해당 정보주체 4. 법률에 특별한 규정이 있거나 법령 상 의무를 준수하기 위하여 이용·제공한 개인정보의 정보주체 5. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 이용·제공한 개인정보의 정보주체 ③ 법 제20조의2제1항에 따라 정보주체에게 통지해야 하는 정보는 다음 각 호와 같다. 1. 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목 2. 개인정보를 제공받은 제3자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정

	보는 제외한다. ④ 법 제20조의2제1항에 따른 통지는 다음 각 호의 어느 하나에 해당하는 방법으로 연 1회 이상 해야 한다. 1. 서면・전자우편・전화・문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법 2. 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법(법 제20조의2제1항에 따른 개인정보의 이용・제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하는 경우로 한정한다)

3. 개정내용 해설

□ 이용·제공 내역 통지 제도가 모든 개인정보처리자로 확대됨에 따라 현실적으로 정보통신서비스 부문 매출액 구분이 어렵고 개인정보와의 관련성이 없는 점을 고려하여 종전 시행령의 매출액 기준은 삭제하여 의무대상에서 제외하였다.

○ 이용・제공 내역 통지 의무대상 기준을 '의무적 수집 출처 통지 대상'의 기준(①5만명 이상 민감·고유식별정보, ②100만명 이상 개인정보)과 동일하게 정비하여 현장에서 혼선이 발생하지 않도록 개선하였다.

□ 정보통신서비스 제공자와 이용자 간의 관계에서 정보주체의 권리 보장을 위해 이용·제공 내역에 대해 알려주도록 한 제도의 취지를 고려하여 통지 대상에서 제외되는 정보주체의 범위를 다음과 같이 명확히 하였다.

○ 첫째, 통지에 대한 거부의사를 표시한 정보주체는 통지 대상에서 제외할 수 있다.

○ 둘째, 개인정보처리자가 업무수행을 위해 소속된 임직원의 개인정보를 처리하거나, 다른 공공기관·법인·단체 등의 임직원에 대한 개인정보를 처리하는 경우에도 통지 대상에서 제외할 수 있다.

○ 셋째, 법률에 특별한 규정이 있거나 법령상 의무준수, 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 이용·제공한 개인정보의 경우 통지 대상에서 제외할 수 있다.

□ 통지의 주기 및 방법은 연 1회 이상 주기적으로 정보주체에게 통지하여야 하며(영 제15조의3제4항), 그 시기는 개인정보처리자가 자유롭게 결정할 수 있다.

○ 한편, 개인정보처리자가 법 제20조제2항에 따라 개인정보의 수집 출처 등에 관한 사항을 알리는 경우 법 제20조의2에 따른 이용·제공 내역의 통지와 함께 통지할 수 있다.(영 제15조의2제3항)

□ 또한, 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 주기적으로 정보주체에게 통지하는 경우에는,

○ 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법을 추가로 활용할 수 있도록 하였다.(영 제15조의3제4항제2호)

< 알림창 예시 >

▸ 개인정보처리자가 기존에 운영하고 있는 사용자 웹사이트(마이페이지 등)에 이용·제공 내역을 확인할 수 있도록 구축하여 운영하고 있는 경우, 알림창 등을 통해 해당 웹사이트 등에서 이용·제공 내역을 확인하는 방법을 안내하는 방법으로 통지 의무를 이행할 수 있음

▸ 이때 알림창은 일정기간 정보주체가 개별적으로 확인할 수 있어야 하므로 앱·웹 내 자체 알림페이지를 통해 안내하는 등의 방식을 활용할 수 있음

※ 개정 전 '수집출처 고지'와 '이용내역 통지' 비교

구분	수집출처 고지(개정전 법 제20조)	이용내역 통지(개정전 법 제39조의8)
도입	'16.3월	'12.2월
대상 사업자	개인정보를 제공받은 개인정보처리자(제3자)로서 ①5만 이상 민감·고유식별 정보 처리 또는 ②100만명 이상 개인정보 처리	정보통신서비스 제공자등으로서 ①이용자수 100만 이상 또는 ②정보통신서비스 부문 매출액 100억 이상
대상 정보	제17조제1항제1호에 따라 정보주체 이외로부터 제공받은 개인정보	제23조, 제39조의3, 제17조에 따라 이용자(정보주체)로부터 수집한 개인정보
통지 항목	수집 출처, 처리 목적, 처리정지권 존재 사실	수집·이용 목적, 수집 항목, 제공받은 자, 제공 목적·항목
방법	제공받은 날로부터 3개월 이내 통지	연 1회 이상 주기적 통지

4. 개인정보처리자 유의사항

□ 법 제20조에 따른 수집 출처 등의 통지와 법 제20조의2에 따른 이용·제공 내역의 통지를 함께 하기 위해서는, 각 규정에서 정보주체에게 알리도록 하는 요구하는 사항을 모두 포함해야 한다.

수집 출처 통지 사항	▸ 개인정보의 수집 출처 ▸ 개인정보의 처리 목적 ▸ 개인정보 처리의 정지를 요구하거나 동의를 철회할 권리가 있다는 사실
이용·제공 내역 통지 사항	▸ 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목 ▸ 개인정보를 제공받은 제3자와 그 제공 목적 및 제공한 개인정보의 항목 (다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외)

□ 이용·제공 내역의 통지는 정보주체가 이용·제공 내역을 개별적으로 확인할 수 있는 상태에 놓이도록 알린 것을 의미하고, 웹사이트 등에 접속하는 모든 이용자에게 일반적으로 공지하는 방법을 의미하지는 않는다는 점에 유의해야 한다.

5. 제재 규정

위반행위	제재 내용
개인정보의 이용・제공 내역이나 이용・제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하지 아니한 자(제20조의2제1항 위반)	3천만원 이하의 과태료 (제75조제2항제3호)

6. 질의 응답

□ 시행령 제15조의2에 따라 수집 출처 통지와 이용·제공 내역 통지를 함께할 수 있음. 제15조의3에 보면 이용·제공 내역 통지는 '정보주체 거부 시 제외'할 수 있도록 하고 있는데, 이러한 제외 조항도 수집 출처 통지에 동일하게 적용할 수 있는지?

⇨ 수집 출처 통지와 이용·제공 내역 통지를 함께할 수 있도록 규정한 것은 동일한 정보주체에게 효율적으로 통지할 수 있도록 통지의 방법을 개선한 것으로, 각 제도의 도입 취지를 고려하면 영 제15조의3의 제외 사유까지 영 제15조의2에 적용하는 것은 아님

※ 법 제20조제2항에 따라 대통령령으로 정하는 개인정보처리자는 정보주체의 요청과 관계없이 수집 출처 등의 통지를 하도록 의무를 부여하고 있음

□ 이용·제공 내역 통지 대상에서 제외할 수 있는 사유 중 공공기관, 법인의 임직원 또는 개인의 연락처 등의 개인정보를 처리한 경우는 어떤 상황을 말하는 것인지?

⇨ 해당 조항의 사례는 B2B 사업 관계에서와 같이 사업자 간 업무 처리를 하는 경우를 말하는 것으로, 이용·제공내역 통지 제도의 도입 목적은 개인정보처리자(사업자)와 정보주체(고객)의 관계에서 정보주체의 권리를 보장하기 위한 조항이므로, 기업 간 이루어지는 B2B 관계에서 업무를 목적으로 업무 상대방의 연락처 등을 처리하는 경우까지 이용·제공 내역을 통지하게 할 필요는 없다는 의견을 반영한 것임

□ 시행령 제15조의3 제2항 제2호에 따르면 '개인정보처리자가 업무수행을 위해 그에 소속된 임직원의 개인정보를 처리한 경우 해당 정보주체'는 법 제20조의2 제1항에 따른 통지의 대상에서 제외되는데, 이에 따라 퇴직자에 대하여도 개인정보 이용.제공 내역을 통지하지 않아도 되는지?

⇨ 비록 퇴사하였다고 하더라도 소속되었던 임직원으로서의 지위에 기반하여 경력증명서 등의 발급을 위해 퇴직 근로자의 개인정보를 보유·이용하는 경우에는 소속된 임직원에 준하여 개인정보를 처리하는 것으로 보아 통지 대상에서 제외할 수 있음

□ 정보주체가 이용·제공 내역 통지에 대한 거부의사를 표시했을 때, 일정 기간 후에 의사를 재확인해야 하는지?

⇨ 통지에 대한 거부의사를 표시한 시점 이후에는 통지 대상에서 제외할 수 있음. 다만, 정보주체가 다시 통지해 줄 것을 요청한 경우에는 그 요청에 따라야 함

□ 이용·제공 내역 통지 내용에 통지를 거부할 수 있다는 설명을 포함해야 하는지?

⇨ 법령상 통지 내용에 포함해야 할 사항은 아니나, 자율적으로 정보주체의 의사를 확인하기 위한 목적으로 포함하여 안내하는 것은 가능함

□ 이용·제공 내역 통지에 대해 거부의사를 전달하는 방법을 반드시 마련하여 안내해야 하는지?

⇨ 통지할 때 통지를 거부할 수 있는 방법을 안내하거나, 개인정보 처리방침에 기재한 개인정보 보호 업무 및 관련 고충사항을 처리하는 부서의 연락처 등을 안내하는 방법 등을 활용하여 안내할 수 있음

□ 수집 출처나 이용·제공 내역 통지를 하는 경우, 정해진 기간(3개월 이내 또는 연1회 이상) 내에 하도록 되어 있음. 그런데 알림창을 통해 통지하면 해당 기간 내에 정보주체가 접속하지 않는 경우가 있을텐데 이 경우 법적 의무 위반인지?

⇨ 정해진 기간 내에 통지하되, 해당 기간이 지나더라도 정보주체가 접속하면 언제든 확인할 수 있도록 알림창을 유지한다면 통지 의무를 이행한 것으로 볼 수 있음

□ 은행이 신용정보법 제35조(신용정보의 이용 및 제공 사실의 조회)에 따라 개인신용정보의 이용 및 제공 사실을 상시적으로 조회할 수 있도록 개인신용정보조회시스템을 구축하고 있는 경우에도 개인정보보호법에 따른 이용·제공내역 통지를 별도로 해야 하는지?

⇨ 은행이 신용정보법 제35조(신용정보 이용 및 제공사실의 조회)에 따라 정보주체가 개인신용정보의 이용 및 제공사실을 조회할 수 있도록 개인신용정보조회시스템을 구축하여 운영하고 있는 개인신용정보에 관해서는 별도로 개인정보보호법에 따른 개인정보 이용·제공 내역 통지를 하지 않아도 됨

다만, 은행이라고 하더라도 개인신용정보 외의 개인정보를 처리하는 경우에는 일반법인 개인정보보호법 제20조의2가 적용되는 점에 유의할 필요가 있음

4 국외 이전 요건 다양화 및 보호조치 강화

1 국외 이전 요건 다양화 (법 제28조의8)

1. 개정 개요

□ 최근 글로벌 서비스 제공자의 출현과, 국가간 전자상거래 확대 등으로 개인정보 국외 이전은 그 중요도와 규모가 지속적으로 증가하고 있고,

○ 기존 법령상의 개인정보 국외 이전 요건이 정보주체의 동의로 한정 되어있어, 데이터의 자유로운 이동을 지향하는 국제규범과의 상호운용성 확보가 필요하다는 지적이 제기되어 왔다.

□ 이에 법 개정을 통해 개인정보의 국외 이전 요건에 보호위원회가 고시하는 개인정보 보호 인증을 받은 경우 또는 보호위원회가 인정한 국가·국제기구로 개인정보를 이전하는 경우를 신설하였다.

2. 법령

법률	**제28조의8(개인정보의 국외 이전)** ① 개인정보처리자는 개인정보를 국외로 제공 (조회되는 경우를 포함한다)·처리위탁·보관(이하 이 절에서 "이전"이라 한다)하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 국외로 이전할 수 있다. 1. 정보주체로부터 국외 이전에 관한 별도의 동의를 받은 경우 2. 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 개인정보의 국외 이전에 관한 특별한 규정이 있는 경우 3. 정보주체와의 계약의 체결 및 이행을 위하여 개인정보의 처리위탁·보관이 필요한 경우로서 다음 각 목의 어느 하나에 해당하는 경우 가. 제2항 각 호의 사항을 제30조에 따른 개인정보 처리방침에 공개한 경우 나. 전자우편 등 대통령령으로 정하는 방법에 따라 제2항 각 호의 사항을 정보주체에게 알린 경우 4. 개인정보를 이전받는 자가 제32조의2에 따른 개인정보 보호 인증 등 보호위원회가 정하여 고시하는 인증을 받은 경우로서 다음 각 목의 조치를 모두 한 경우 가. 개인정보 보호에 필요한 안전조치 및 정보주체 권리보장에 필요한 조치 나. 인증받은 사항을 개인정보가 이전되는 국가에서 이행하기 위하여 필요한 조치 5. 개인정보가 이전되는 국가 또는 국제기구의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 보호위원회가 인정하는 경우 ② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 미리 다음 각 호의 사항을 정보주체에게 알려야 한다. 1. 이전되는 개인정보 항목

	2. 개인정보가 이전되는 국가, 시기 및 방법 3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭과 연락처를 말한다) 4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간 5. 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과 ③ 개인정보처리자는 제2항 각 호의 어느 하나에 해당하는 사항을 변경하는 경우에는 정보주체에게 알리고 동의를 받아야 한다. ④ 개인정보처리자는 제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우 국외 이전과 관련한 이 법의 다른 규정, 제17조부터 제19조까지의 규정 및 제5장의 규정을 준수하여야 하고, 대통령령으로 정하는 보호조치를 하여야 한다. ⑤ 개인정보처리자는 이 법을 위반하는 사항을 내용으로 하는 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다. ⑥ 제1항부터 제5항까지에서 규정한 사항 외에 개인정보 국외 이전의 기준 및 절차 등에 필요한 사항은 대통령령으로 정한다.
시행령	**제29조의7(개인정보의 국외 처리위탁·보관 시 정보주체에게 알리는 방법)** 법 제28조의8제1항제3호나목에서 "전자우편 등 대통령령으로 정하는 방법"이란 서면등의 방법을 말한다. **제29조의8(개인정보의 국외 이전 인증)** ① 보호위원회는 법 제28조의8제1항제4호 각 목 외의 부분에 따른 인증을 고시하려는 경우에는 다음 각 호의 순서에 따른 절차를 모두 거쳐야 한다. 1. 제34조의6에 따른 개인정보 보호 인증 전문기관의 해당 인증에 대한 평가 2. 국외이전전문위원회의 평가 3. 정책협의회의 협의 ② 보호위원회는 법 제28조의8제1항제4호 각 목 외의 부분에 따른 인증을 고시할 때에는 5년의 범위에서 유효 기간을 정하여 고시할 수 있다. ③ 제1항 및 제2항에서 규정한 사항 외에 인증의 고시 절차 등에 관하여 필요한 사항은 보호위원회가 정하여 고시한다. **제29조의9(국가 등에 대한 개인정보 보호 수준 인정)** ① 보호위원회는 법 제28조의8제1항제5호에 따라 개인정보가 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 장에서 "이전"이라 한다)되는 국가 또는 국제기구(이하 "이전대상국등"이라 한다)의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 인정하려는 경우에는 다음 각 호의 사항을 종합적으로 고려해야 한다. 1. 이전대상국등의 법령, 규정 또는 규칙 등 개인정보 보호체계가 법 제3조에서 정하는 개인정보 보호 원칙에 부합하고, 법 제4조에서 정하는 정보주체의 권리를 충분히 보장하고 있는지 여부 2. 이전대상국등에 개인정보 보호체계를 보장하고 집행할 책임이 있는 독립적 감독기관이 존재하는지 여부 3. 이전대상국등의 공공기관(이와 유사한 사무를 수행하는 기관을 포함한다)이 법률에 따라 개인정보를 처리하는지 여부 및 이에 대한 피해구제 절차 등 정보주체에 대한 보호수단이 존재하고 실질적으로 보장되는지 여부 4. 이전대상국등에 정보주체가 쉽게 접근할 수 있는 피해구제 절차가 존재하는지 여부 및 피해구제 절차가 정보주체를 효과적으로 보호하고 있는지 여부 5. 이전대상국등의 감독기관이 보호위원회와 정보주체의 권리 보호에 관하여 원활한 상호 협력이 가능한지 여부 6. 그 밖에 제1호부터 제5호까지에 준하는 사항으로서 보호위원회가 정하여 고시하는 사항

	② 보호위원회는 제1항에 따른 인정을 하려는 경우에는 다음 각 호의 절차를 거쳐야 한다. 1. 국외이전전문위원회의 평가 2. 정책협의회의 협의 ③ 보호위원회는 제1항에 따른 인정을 할 때에는 정보주체의 권리 보호 등을 위하여 필요한 경우 이전대상국등으로 이전되는 개인정보의 범위, 이전받는 개인정보처리자의 범위, 인정 기간, 국외 이전의 조건 등을 이전대상국등별로 달리 정할 수 있다. ④ 보호위원회는 제1항에 따른 인정을 한 경우에는 인정 기간 동안 이전대상국등의 개인정보 보호수준이 법에 따른 수준과 실질적으로 동등한 수준을 유지하고 있는지 점검해야 한다. ⑤ 보호위원회는 제1항에 따른 인정을 받은 이전대상국등의 개인정보 보호체계, 정보주체의 권리보장 범위, 피해구제 절차 등의 수준이 변경된 경우에는 해당 이전대상국등의 의견을 듣고 해당 이전대상국등에 대한 인정을 취소하거나 그 내용을 변경할 수 있다. ⑥ 보호위원회가 제1항에 따른 인정을 하였거나 제5항에 따라 인정을 취소하거나 그 내용을 변경하는 경우에는 그 사실을 관보에 고시하고 보호위원회 인터넷 홈페이지에 게재해야 한다. ⑦ 제1항부터 제6항까지에서 규정한 사항 외에 이전대상국등에 대한 인정에 관하여 필요한 사항은 보호위원회가 정하여 고시한다. **제29조의10(개인정보의 국외 이전 시 보호조치 등)** ① 개인정보처리자는 법 제28 조의8제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우에는 같은 조 제4항에 따라 다음 각 호의 보호조치를 해야 한다. 1. 제30조제1항에 따른 개인정보 보호를 위한 안전성 확보 조치 2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치 3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 조치 ② 개인정보처리자는 법 제28조의8제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하려는 경우에는 제1항 각 호의 사항에 관하여 이전받는 자와 미리 협의하고 이를 계약내용 등에 반영해야 한다.

3. 개정내용 해설

□ 온라인(정보통신서비스 제공자)과 오프라인을 구분하여 달리 규율하고 있던 개인정보 국외 이전 규정을 하나의 조항으로 일원화하여,

○ 모든 개인정보처리자는 개인정보의 국외 이전과 관련하여 동일한 법령상 의무(국외 이전 요건, 보호조치 등)를 준수하여야 한다.

□ 개인정보 국외 이전 요건에 ▲보호위원회가 고시하는 개인정보 국외 이전 인증을 받은 경우(법 제28조의8제1항제4호)와, ▲이전받는 국가·국제기구의 개인정보 보호 수준이 우리 법에 따른 개인정보 보호 수준과 같다고 인정하는 경우(법 제28조의8제1항제5호)를 추가하였다.

○ 이에 따라 보호위원회가 고시하는 인증을 획득한 자나, 개인정보 보호 수준이 동등하다고 보호위원회가 인정한 국가 또는 국제기구로의 개인정보 국외 이전은 정보주체의 별도 동의 없이 가능하도록 하였다.

< 관련 사례 1 >

▸ 해외기업이 법 제32조의2에 따른 개인정보 보호 인증(ISMS-P)을 취득한 경우, 법 제28조의8제1항 제4호에 따라 국내기업에서 해당 해외기업으로 개인정보를 제공(조회되는 경우 포함)·처리위탁·보관할 때 개인정보의 국외 이전에 관한 정보주체의 별도 동의 획득이 불필요

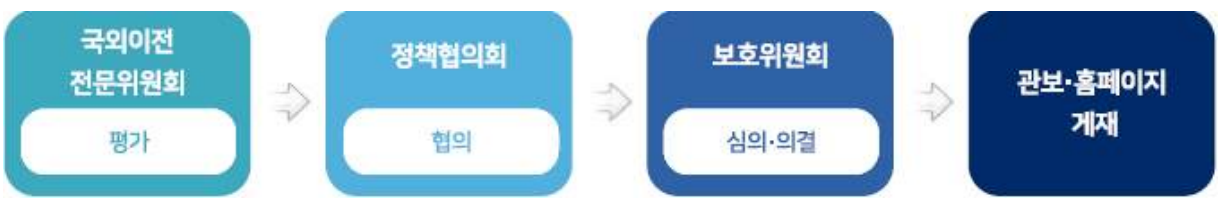
< 관련 사례 2 >

▸ 보호위원회는 개인정보 국외 이전 대상국 후보로 A국가를 선정하고 개인정보 보호 수준을 검토한 결과 A국의 개인정보 보호 수준이 국내법과 동등하다고 인정하였다. 이에 따라, 정보주체의 동의를 통해 국외로 개인정보를 이전하고 있던 기업은 향후 국외 이전에 관한 정보주체의 별도 동의 없이도 A국가의 개인정보처리자에게 개인정보 이전이 가능하게 됨

○ 법 개정 전후 비교 및 운영절차

구분		법 개정 전		법 개정 후
개인정보 국외이전	대상	개인정보처리자 (법 제17조③)	정보통신서비스 제공자등 (법 제39조의12)	개인정보처리자(법 제28조의8) (온·오프라인 통합)
	요건	· 국외 제3자 제공 시 정보주체의 동의	· 국외 이전* 시 정보주체의 동의 * 제공(조회 포함)·처리위탁·보관	· 국외 이전* 시 정보주체의 동의 * 제공(조회 포함)·처리위탁·보관
			· 처리위탁·보관의 경우 개인정보 처리방침 공개 시 동의 대체	· 계약체결 및 이행을 위해 처리위탁·보관이 필요한 경우로서 개인정보 처리방침에 공개한 경우 · 보호위원회가 정하여 고시한 인증을 받은 경우 · 국가 또는 국제기구의 보호수준을 보호위원회가 인정한 경우

- 개인정보 국외 이전 인증 절차 -



- 국가 등에 대한 개인정보 보호 수준 인정 절차 -

4. 개인정보처리자 유의사항

□ 법 제28조의8제1항 각호의 개인정보 국외 이전 요건을 충족하는 것과 별개로, 개인정보를 수집하여 이용하거나, 수집한 개인정보를 제3자에게 제공하는 등 개인정보를 처리하는 경우 우리 법상의 관련 조항에 따라 정보주체의 동의를 획득하는 등 적법한 절차를 준수하여야 한다.

* 국외 이전과 관련한 이 법의 다른 규정, 제17조부터 제19조까지의 규정, 제5장의 규정, 대통령령으로 정하는 보호조치 등

< 관련 사례 >

▸ C社는 해외에 소재하고 있으며, C社가 소재한 국가는 보호위원회로부터 개인정보 보호 수준을 인정받은 국가임. 또한, 국내기업 D社는 마케팅 활용 등을 목적으로 정보주체로부터 동의를 받아 보유하고 있는 개인정보를 해외 소재 C社에게 제공하고자 함. 이 경우 개인정보를 국외로 이전하기 위한 동의는 불필요하나, 제3자에게 제공하기 위한 동의(제17조 또는 제18조)는 받아야 함

◈ 국외 이전에 대한 인정 및 인증, 중지 명령 등에 대한 세부 절차를 정한「개인정보 국외이전 운영 등에 관한 규정」고시 참고

5. 제재 규정

위반행위	제재 내용
법 제28조의8제1항을 위반하여 개인정보를 국외로 이전한 경우(제26조제8항 및 제28조의11에 따라 준용되는 경우 포함)	과징금 부과 (제64조의2제1항제7호)
법 제28조의8제4항을 위반하여 보호조치를 하지 아니한 자 (제26조제8항 및 제28조의11에 따라 준용되는 경우 포함)	3천만원 이하의 과태료 부과 (제75조제2항제14호)

6. 질의 응답

□ 법 제28조의8제1항제3호의 ‘정보주체와의 계약체결 및 이행을 위해’란 어떤 경우를 말하는 것인지?

⇨ 정보주체와의 계약체결 및 이행을 위해 필요한 경우는 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우로서, 국외에서 개인정보 처리위탁이 필요하거나 국외에서 개인정보 보관이 필요한 경우를 의미함

다만 특정 업무가 정보 주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우인지 여부는 해당 사업자가 제공하는 서비스·제품의 성격 및 사업 구조 등을 종합적으로 고려하여 판단이 필요

□ 개인정보 보호와 관련된 인증은 아무거나 보유하고 있으면 정보 주체의 동의 없이 국외 이전이 가능한지?

⇨ 이전받는 자가 법 제32조의2에 따른 개인정보 보호 인증(ISMS-P) 등 보호위원회가 정하여 고시하는 인증을 받은 경우로서, 제28조의8제1항제4호 각 목의 조치*들을 이행한 경우에 한정하고 있음

* ㉮개인정보 보호에 필요한 안전조치 및 정보주체 권리보장에 필요한 조치, ㉯인증받은 사항을 개인정보가 이전되는 국가에서 이행하기 위하여 필요한 조치

□ 개인정보를 이전받는 기업의 개인정보 국외 이전 인증이 갱신되지 않는 경우에는 어떻게 되는지?

⇨ 국외 이전을 위해서는 법 제28조의8제1항에 명시된 국외 이전 요건 중 어느 하나에 해당하여야 하므로, 개인정보를 이전받는 자의 인증이 만료된 경우 다른 국외 이전 요건을 준수하거나, 국외 이전을 중단해야 함

□ 개인정보 국외 이전 인증, 국외 이전이 가능한 이전대상국등 인정에 대한 검토는 신청하는 별도의 절차가 있는지? 향후 검토 일정은 어떻게 되는지?

⇨ 개인정보 국외 이전 인증 및 국외 이전이 가능한 이전대상국등에 대한 인정은 별도의 신청 절차를 두고 있지 않으며, 상대 국가·기관 등과의 협의 진척 수준, 경제적 효과 및 기타 정책적 고려사항을 바탕으로 순차적으로 검토에 착수할 계획임

□ 법 제22조제1항 각 호에 구분하여 동의를 받아야 하는 사항 중 '제28조의8제1항에 따라 동의를 받는 경우'는 규정하고 있지 않은데, 제3자 제공 동의 받을 때 국외 이전 동의도 함께 명시하여 하나로 동의를 받아도 되는지?

⇨ 법 제28조의8제1항제1호에 따르면 국외이전에 관한 동의는 정보주체로부터 별도로 받도록 하고 있으며, 이에 따라 법 제17조·제18조에 따른 제3자 제공 동의와 제28조의8제1항제1호의 국외 이전에 관한 동의는 별도로 구분하여 받아야 함

□ 개인정보를 동의를 받아 국외로 제3자 제공을 하는 경우, 국외 이전 동의와 제3자 동의를 둘 다 받아야 하는지?

⇨ 법 제17조·제18조에 따른 제3자 제공 동의와 제28조의8제1항제1호의 국외 이전에 관한 동의는 별도로 구분하여 받아야 함

⇨ 다만, 법 제17조제4항에 따라 당초 수집 목적과 합리적으로 관련된 범위에서는 정보주체의 동의 없이도 개인정보를 제공할 수 있으므로, 국외이전에 관한 동의만 받아 제공할 수 있음.

※ 법 제17조제4항에 따른 추가적 제공에 관하여 자세한 사항은 7p 참고

2 국외 이전 중지 명령 (법 제28조의9)

1. 개정 개요

□ 개인정보 국외 이전 요건 확대와 함께, 개인정보 국외 이전으로 인해 정보주체의 피해가 예상되는 경우 피해예방을 위한 제도적 안전망 구축의 필요성이 제기되었다.

□ 이번 법 개정으로 개인정보 국외 이전 관련 규정을 위반하거나 개인정보 보호 수준이 취약하여 국외 이전시 정보 주체의 피해가 우려될 때는, 개인정보 국외 이전 중지를 명령할 수 있도록 하여 정보 주체의 피해를 예방할 수 있도록 하였다.

2. 법령

법률	**제28조의9(개인정보의 국외 이전 중지 명령)** ① 보호위원회는 개인정보의 국외 이전이 계속되고 있거나 추가적인 국외 이전이 예상되는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 개인정보의 국외 이전을 중지할 것을 명할 수 있다. 1. 제28조의8제1항, 제4항 또는 제5항을 위반한 경우 2. 개인정보를 이전받는 자나 개인정보가 이전되는 국가 또는 국제기구가 이 법에 따른 개인정보 보호 수준에 비하여 개인정보를 적정하게 보호하지 아니하여 정보주체에게 피해가 발생하거나 발생할 우려가 현저한 경우 ② 개인정보처리자는 제1항에 따른 국외 이전 중지 명령을 받은 경우에는 명령을 받은 날부터 7일 이내에 보호위원회에 이의를 제기할 수 있다. ③ 제1항에 따른 개인정보 국외 이전 중지 명령의 기준, 제2항에 따른 불복 절차 등에 필요한 사항은 대통령령으로 정한다.
시행령	**제29조의11(국외 이전 중지 명령의 기준 등)** ① 보호위원회는 법 제28조의9제1항에 따라 개인정보의 국외 이전을 중지할 것을 명하려는 경우에는 다음 각 호의 사항을 종합적으로 고려해야 한다. 1. 국외로 이전되었거나 추가적인 국외 이전이 예상되는 개인정보의 유형 및 규모 2. 법 제28조의8제1항, 제4항 또는 제5항 위반의 중대성 3. 정보주체에게 발생하거나 발생할 우려가 있는 피해가 중대하거나 회복하기 어려운 피해인지 여부 4. 국외 이전의 중지를 명하는 것이 중지를 명하지 않는 것보다 명백히 정보주체에게 이익이 되는지 여부 5. 법 제64조제1항에 따른 시정조치를 통해 개인정보의 보호 및 침해 방지가 가능한지 여부 6. 개인정보를 이전받는 자나 개인정보가 이전되는 이전대상국등이 정보주체의 피해구제를 위한 실효적인 수단을 갖추고 있는지 여부 7. 개인정보를 이전받는 자나 개인정보가 이전되는 이전대상국등에서 중대한 개인정보 침해가

	발생하는 등 개인정보를 적정하게 보호하기 어렵다고 인정할 만한 사유가 존재하는지 여부 ② 보호위원회는 법 제28조의9제1항에 따라 개인정보의 국외 이전을 중지할 것을 명하려는 경우에는 국외이전전문위원회의 평가를 거쳐야 한다. ③ 보호위원회는 법 제28조의9제1항에 따라 개인정보의 국외 이전을 중지할 것을 명할 때에는 개인정보처리자에게 중지명령의 내용, 사유, 이의 제기 절차·방법 및 그 밖에 필요한 사항을 문서로 알려야 한다. ④ 제1항부터 제3항까지에서 규정한 사항 외에 국외 이전 중지 명령의 기준 등에 필요한 세부사항은 보호위원회가 정하여 고시한다. **제29조의12(국외 이전의 중지 명령에 대한 이의 제기)** ① 법 제28조의9제2항에 따라 이의를 제기하려는 자는 같은 조 제1항에 따른 국외 이전 중지 명령을 받은 날부터 7일 이내에 보호위원회가 정하는 이의신청서에 이의신청 사유를 증명할 수 있는 서류를 첨부하여 보호위원회에 제출해야 한다. ② 보호위원회는 제1항에 따라 이의신청서를 제출받은 날부터 30일 이내에 그 처리결과를 해당 개인정보처리자에게 문서로 알려야 한다. ③ 제1항 및 제2항에서 규정한 사항 외에 이의 제기의 절차 등에 필요한 사항은 보호위원회가 정하여 고시한다.

3. 개정내용 해설

□ 보호위원회는 개인정보처리자가 개인정보를 국외 이전 시 법률(제28조의8 제1항, 제4항 또는 제5항)을 위반하거나, 개인정보를 이전하는 또는 이전받는 자가 적정하게 개인정보를 보호하지 아니하여 정보주체에게 피해가 발생하거나 발생할 우려가 현저한 경우 해당 개인정보처리자에게 국외 이전 중지를 명할 수 있다.

○ 보호위원회는 전체회의를 통해 이전이 제한되는 개인정보 유형, 이전이 제한되는 국가, 중지 명령 사유 등을 의결하고, 해당 개인정보처리자에게 국외 이전 중지 명령을 통보해야 한다.

□ 국외 이전 중지를 명령받은 개인정보처리자는 이에 불복하는 경우, 명령을 받은 날부터 7일 이내에 이를 증빙하는 서류를 첨부하여 보호위원회에 제출하는 방식으로 이의를 제기할 수 있는데,

○ 보호위원회는 이의 제기내용에 대해 검토하여 30일 이내에 처리결과를 해당 개인정보처리자에게 통보해야 한다.

< 관련 사례 1 >

▸ 개인정보 보호 인증(ISMS-P)을 받은 해외기업은 국내 정보주체의 국외 이전 동의 없이 개인정보를 국외로 이전받고 있었음. 그런데 ISMS-P 인증기간이 만료되어 인증 효력이 상실되었으나, 계속 개인정보를 국외로 이전하고 있었음. 이 경우 개인정보 국외 이전 중지 명령 대상이 될 수 있음

< 관련 사례 2 >

▸ 국내기업이 개인정보 국외 이전 인정을 받은 국가에 있는 해외기업으로 개인정보를 이전하는 과정에서 개인정보처리자 및 개인정보를 이전받는자가 개인정보 보호에 필요한 안전조치를 누락한 사실이 확인됨. 이 경우 국외 이전 중지 명령 대상이 될 수 있음

◈ 국외 이전에 대한 인정 및 인증, 중지 명령 등에 대한 세부 절차는「개인정보 국외 이전 운영 등에 관한 규정」고시 참고

4. 개인정보처리자 유의사항

□ 국외 이전 중지를 명령받은 개인정보처리자는 당초의 중지 명령 사유가 해소되었을 때 중지 명령 해제를 신청할 수 있다.

5. 제재 규정

위반행위	제재 내용
제28조의9제1항을 위반하여 국외 이전 중지 명령을 따르지 아니한 경우 (제26조제8항 및 제28조의11에 따라 준용되는 경우 포함)	과징금 부과 (제64조의2제1항제8호)

6. 질의 응답

□ 국외 이전 중지 명령에 대해 이의를 제기한 후 보호위원회로부터 이의제기 결과를 통보받기 전이라면 개인정보의 국외 이전을 중단하지 않아도 되는지?

⇨ 국외 이전 중지명령은 권한이 있는 기관이 취소 또는 철회하거나 기간의 경과 등으로 소멸되기 전까지는 유효한 것으로 통용되며(행정기본법 제15조), 법령에 별도의 규정이 없는 한 이의제기로 인하여 그 집행이 정지되지 않음. 개정 개인정보보호법 제28조의9에서는 집행정지에 관한 규정을 두고 있지 않으므로 보호위원회에 국외 이전 중지명령에 대한 이의가 제기되더라도 중지명령의 효력, 집행 또는 절차의 속행에 영향을 주지 않음

□ 국외 이전 중지 명령을 받는 즉시 개인정보의 국외 이전을 중단하여야 하는지?

⇨ 국외 이전 중지 명령 시 구체적인 중지 시점을 명시할 계획이며, 개인정보 국외 이전 중지명령이 발효되면 즉시 개인정보 국외 이전을 중지하여야 함

□ 국외 이전 중지 명령은 어떻게 해제될 수 있는지?

⇨ 국외 이전 중지 명령에 대한 사유가 해소되면, 해당 개인정보처리자는 보호위원회에 중지 명령 해제신청서를 제출함으로써 해제를 요청할 수 있음
보호위원회는 중지 명령의 해제를 요청받은 경우 중지 명령 사유가 해소되었는지를 검토하고 보호위원회의 심의·의결을 거쳐 중지 명령이 해제되었음을 해당 개인정보처리자에게 통보함으로써 중지 명령이 해제됨

□ 국외 이전 중지 명령권 발동을 위한 조사 개시는 어떤 방식으로 이루어지는지?

⇨ 국외 이전 중지를 명하기 위한 사실 조사와 처분은 위법 사항이 발견되어 국외 이전으로 인한 정보주체의 권리 침해 우려가 현저한 개인정보처리자를 중심으로 이루어질 전망임

□ 법 제28조의9(개인정보의 국외 이전 중지 명령)에서 언급한 정보주체에게 피해가 발생될 우려가 '현저한' 경우는 어떻게 판단하는지?

⇨ 법령 위반의 정도, 예상되는 정보주체의 피해 규모, 기타 수단을 통한 해소 가능성 등을 종합 고려하여 국외이전전문위원회를 통해 전문가 의견을 바탕으로 판단할 계획임

참고 **개인정보 국외 이전 운영 등에 관한 규정('23.10.16. 시행)**

제1장 총칙

제1조(목적) 이 고시는 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제5조, 제29조의8, 제29조의9, 제29조의11, 제29조의12에 따라 개인정보의 국외 이전에 관하여 필요한 사항을 정함을 목적으로 한다.

제2조(정의) 이 고시에서 사용하는 용어의 정의는 다음과 같다.

1. "국외이전전문위원회"는 영 제5조제1항에 따라 개인정보 보호 관련 전문가 등으로 구성된 개인정보 국외 이전 분야의 전문위원회를 말한다.
2. "개인정보 국외 이전 인증"이란 영 제29조의8제1항에 따라 개인정보 보호위원회(이하 "보호위원회"라 한다)가 고시하는 인증을 말한다.
3. "개인정보 보호 인증 전문기관"이란 영 제34조의6에 따른 개인정보 보호 인증 전문기관을 말한다.
4. "이전대상국등"이란 법 제28조의8제1항제5호에 따라 개인정보가 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 '이전'이라 한다)되는 국가 또는 국제기구를 말한다.

제2장 국외이전전문위원회 운영 등

제3조(국외이전전문위원회 위원의 임기) 국외이전전문위원회 위원(이하 '위원'이라 한다)의 임기는 위촉된 날로부터 3년으로 하되 연임할 수 있다. 다만, 영 제5조제2항제1호에 해당하는 위원의 임기는 해당 직위에 재직하는 기간으로 한다.

제4조(국외이전전문위원회 운영) ① 국외이전전문위원회 회의는 보호위원회의 요청에 따라 국외이전전문위원회 위원장이 소집한다.

② 국외이전전문위원회 위원장이 부득이한 사유로 그 직무를 수행할 수 없는 때에는 국외이전전문위원회 위원장이 미리 지명한 위원이 그 직무를 대행한다.

③ 국외이전전문위원회는 재적위원 과반수의 출석으로 개회하고 출석위원 과반수의 찬성으로 의결한다.

④ 국외이전전문위원회는 필요한 경우 관계기관의 공무원 및 이해관계인에게 국외이전전문위원회 회의 출석 또는 의견 제출을 요청할 수 있다.

⑤ 국외이전전문위원회 회의는 공개하지 않는다. 다만, 다음 각 호의 사항을 포함한 회의록을 작성하여 보관하여야 하며, 국외이전전문위원회 위원장이 필요하다고 인정하면 녹음 또는 녹화를 할 수 있다.

1. 회의 일시 및 장소
2. 회의에 참석한 위원 명단
3. 회의 안건 및 내용

⑥ 국외이전전문위원회 위원장이 안건을 검토한 결과 사안이 긴급을 요하거나 토론을 요하지 아니한다고 판단되는 경우, 국외이전전문위원회 회의를 서면으로 개최할 수 있다.

제5조(간사 등) ① 국외이전전문위원회에 간사 1인을 두되, 간사는 보호위원회 사무처 소속 공무원 중에서 개인정보의 국외 이전 업무를 담당하는 부서의 장이 된다.

② 간사는 다음 각 호의 업무를 수행한다.

1. 국외이전전문위원회 위원장의 국외이전전문위원회 운영에 관한 보좌
2. 국외이전전문위원회 회의록 작성 및 보관
3. 국외이전전문위원회의 업무에 관한 사무처리 등

제6조(소위원회) 국외이전전문위원회 위원장은 국외이전전문위원회 업무를 효율적으로 수행하기 위하여 필요하다고 인정될 경우 일부 위원으로 구성되는 소위원회를 둘 수 있다.

제7조(위원의 제척 사유) 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 평가에 관여하지 못한다

1. 위원 본인과 직접적인 이해관계가 있는 사항

2. 위원 본인과 친족관계에 있거나 있었던 자와 관련된 사항
3. 위원이 해당 사안에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 해당 사안에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우
5. 위원이나 위원이 속한 공공기관·법인 또는 단체 등이 조언 등 지원을 하고 있는 자와 이해관계가 있는 경우

제8조(위원의 해임 및 해촉) 보호위원회 위원장은 위원이 다음 각 호의 어느 하나에 해당하는 경우에는 해당 위원을 해임 또는 해촉할 수 있다.
1. 심신장애로 인하여 직무를 수행할 수 없게 된 경우
2. 직무와 관련된 비위사실이 있는 경우
3. 직무 태만, 품위 손상, 그 밖의 사유로 인하여 위원의 직을 유지하는 것이 적합하지 아니하다고 인정되는 경우
4. 위원 스스로 직무를 수행하는 것이 곤란하다고 의사를 밝히는 경우

제9조(수당과 여비) 국외이전전문위원회와 제6조에 따른 소위원회의 회의에 출석한 위원 등에게는 예산의 범위에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 그 소관 업무와 직접적으로 관련되어 출석하는 경우에는 그러하지 아니하다.

제10조(운영세칙) 국외이전전문위원회의 운영에 관하여 이 규정에서 정하지 아니한 세부적 사항은 국외이전전문위원회의 의결을 거쳐 국외이전전문위원회 위원장이 정한다.

제3장 개인정보 국외 이전 인증

제11조(인증에 대한 개인정보 보호 인증 전문기관의 평가) 개인정보 보호 인증 전문기관이 영 제29조의8제1항제1호에 따라 평가를 할 때에는 별표1의 기준에 따라 해당 인증의 개인정보 보호 수준, 정보주체의 권리 보호 적절성 등을 평가하고 그 내용을 보호위원회에 제출하여야 한다.

제12조(인증에 대한 국외이전전문위원회의 평가) 국외이전전문위원회가 영 제29조의8제1항제2호에 따라 평가를 할 때에는 별표1의 기준에 따라 해당 인증의 개인정보 보호 수준, 정보주체의 권리 보호 적절성 등을 평가하고 그 내용을 보호위원회에 제출하여야 한다.

제13조(인증에 대한 정책협의회의 협의) 보호위원회는 영 제29조의8제1항제3호에 따라 정책협의회를 개최하여 해당 인증에 대하여 관계기관과 협의하여야 한다.

제14조(인증에 대한 보호위원회 심의·의결) 보호위원회는 제11조에 따른 개인정보 보호 인증 전문기관 평가 내용, 제12조에 따른 국외이전전문위원회 평가 내용, 제13조에 따른 정책협의회 협의 내용 등을 종합적으로 고려하여, 보호위원회의 심의·의결을 거쳐 법 제28조의8제1항제4호에 따라 고시하는 인증을 정한다.

제15조(개인정보 국외 이전 인증) 제14조에 따라 보호위원회가 정하는 인증은 별표2와 같다.

제16조(유효기간과 갱신) ① 보호위원회는 영 제29조의8제2항에 따른 유효기간 만료 전에 해당 인증의 유효기간 갱신 여부를 심의하고, 이를 갱신할 수 있다.
② 제1항에 따른 심의를 하려는 경우 제11조부터 제14조까지의 절차를 거쳐야 한다.

제17조(인증의 제외) 보호위원회는 이 장에 따라 고시한 인증의 개인정보 보호 수준이 법 제32조의2에 따른 개인정보 보호 인증의 개인정보 보호 수준에 미치지 못한다고 판단하는 경우 해당 인증에 대해 제11조부터 제14조까지의 절차를 거쳐 해당 인증을 별표2에서 제외할 수 있다.

제4장 국가 등에 대한 개인정보 보호 수준 인정

제18조(이전대상국등 인정에 대한 국외이전전문위원회 평가) 국외이전전문위원회가 영 제29조의9제2항에 따라 평가를 할 때에는 영 제29조의9제1항 각 호의 사항에 따라 이전대상국등의 개인정보 보호 수준, 정보주체의 권리 보호 적절성 등을 평가하고 평가 내용을 보호위원회에 제출하여야 한다.

제19조(이전대상국등 인정에 대한 정책협의회의 협의) 보호위원회는 영 제29조의9제2항제2호에 따라 정책협의회를 개최하여 해당 이전대상국등 인정에 대해 관계기관과 협의하여야 한다.

제20조(이전대상국등 인정에 대한 보호위원회 심의·의결) 보호위원회는 제18조에 따른 국외이전전문위원회 평가 내용 및 제19조에 따른 정책협의회 협의 내용 등을 종합적으로 고려하여, 보호위원회의 심의·의결을 거쳐 법 제28조의8제1항제5호에 따라 이전대상국등의 인정 여부를 정한다.

제21조(이전대상국등 인정기간 및 갱신) ① 보호위원회는 영 제29조의9제3항에 따른 이전대상국등의 인정 기간 만료 전에 갱신 여부를 심의하고, 이를 연장할 수 있다.

② 제1항에 따른 심의를 하려는 경우 제18조부터 제20조까지의 절차를 거쳐야 한다.

제22조(이전대상국등 인정의 내용변경 및 취소 등) 보호위원회는 영 제29조9제5항에 따라 인정을 취소하거나 그 내용을 변경할 경우에는 해당 이전대상국등의 의견을 듣고 제18조부터 제20조까지의 절차를 거쳐야 한다.

제5장 개인정보 국외 이전 중지 명령

제23조(국외 이전 중지 명령에 대한 국외이전전문위원회 평가 등) 국외이전전문위원회가 영 제29조의11제2항에 따른 평가를 할 때에는 영 제29조의11제1항 각 호의 사항에 따라 법령 위반의 중대성, 피해의 심각성 등을 평가하고 평가 내용을 보호위원회에 제출하여야 한다.

제24조(국외 이전 중지 명령에 대한 보호위원회 심의·의결) ① 보호위원회는 국외이전전문위원회 평가 내용 등을 고려하여 보호위원회의 심의·의결을 거쳐 해당 개인정보처리자에 대한 개인정보 국외 이전 중지를 명한다.

② 보호위원회는 중지 명령 심의에 필요한 경우 해당 개인정보처리자에게 관련 자료를 요청할 수 있다.

제25조(국외 이전 중지 명령의 통보 등) 영 제29조의11제3항에 따라 개인정보처리자에게 국외 이전 중지를 명하는 문서는 별지 제1호 서식에 따른다.

제26조(국외 이전 중지 명령 이의 제기 등) ① 영 제29조의12제1항에 따라 보호위원회가 정하는 이의신청서는 별지 제2호의 서식에 따른다.

② 보호위원회는 제1항에 따른 중지 명령 이의제기를 받은 경우에는 30일 이내에 중지 명령 해제 여부를 결정하고 그 내용을 신청인에게 문서로 알려야 한다.

제27조(국외 이전 중지 명령의 해제) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우 개인정보의 국외 이전 중지 명령을 해제할 수 있다.

1. 보호위원회가 법 제28조의9제1항 각 호의 어느 하나에 해당하지 않는다고 인정하는 경우
2. 보호위원회가 개인정보처리자의 법 제28조의9제2항에 따른 이의제기가 정당하다고 인정하는 경우
3. 그 밖에 보호위원회가 필요하다고 인정하는 경우

② 법 제28조의9에 따라 국외 이전의 중지를 명령받은 개인정보처리자가 제1항제1호에 따라 중지 명령의 해제를 요청하려는 경우에는 별지 제3호의 서식과 이를 증명하는데 필요한 서류를 첨부하여 보호위원회에 제출하여야 한다.

③ 보호위원회는 제1항에 따라 중지 명령을 해제할 때에는 해당 개인정보처리자에게 문서로 알려야 한다.

제6장 보 칙

제28조(재검토기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2023년 9월 15일 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-11호, 2023. 10. 16.>

이 고시는 공포한 날부터 시행한다.

※ 별표 및 별지 서식은 국가법령정보센터(www.law.go.kr) 참조

5 안전조치 의무 일원화 및 공공기관 안전조치 강화

1 안전성 확보 조치 (영 제30조)

1. 개정 개요

□ 법 개정으로 정보통신서비스 제공자에 대한 특례규정이 삭제됨에 따라 개인정보의 안전조치 관련 일반규정(종전 영 제30조)과 정보통신서비스 제공자에 대한 특례규정(종전 영 제48조의2)을 일반규정(개정 영 제30조)으로 통합하여 정비하였다.

□ 안전조치 기준이 모든 개인정보처리자에게 동일하게 적용될 수 있도록 일원화하였다.

○ 클라우드 확산, 인증수단 다양화 등 기술환경 변화를 반영하고, 개인정보의 안전조치를 위한 다양한 기술이 도입될 수 있도록 특정 기술에 종속적인 규정을 기술중립적으로 변경하였고,

○ 암호화 대상, 접근통제, 내부 관리계획 등 일반규정과 특례규정 간 유사·상이한 조항은 정보주체의 권리보호를 우선하여 통합하되 기술변화 및 사업자에게 미치는 영향의 정도 등을 종합적으로 고려하여 합리적으로 개선하였다.

2. 법령

법률	**제29조(안전조치의무)** 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
시행령	**제30조(개인정보의 안전성 확보 조치)** ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. 1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부 관리계획의 수립·시행 및 점검 가. 법 제28조제1항에 따른 개인정보취급자(이하 "개인정보취급자"라 한다)에 대한 관리·감독 및 교육에 관한 사항 나. 법 제31조에 따른 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항 다. 제2호부터 제8호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항 2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치 가. 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행 나. 정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한 인증수단 적용 기준의 설정 및 운영 다. 그 밖에 개인정보에 대한 접근 권한을 제한하기 위하여 필요한 조치 3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치

	가. 개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치 나. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단. 다만, 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제1항제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당한다. 다. 그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치 4. 개인정보를 안전하게 저장·전송하는데 필요한 다음 각 목의 조치 가. 비밀번호의 일방향 암호화 저장 등 인증정보의 암호화 저장 또는 이에 상응하는 조치 나. 주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장 또는 이에 상응하는 조치 다.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제1항제1호에 따른 정보통신망을 통하여 정보주체의 개인정보 또는 인증정보를 송신·수신하는 경우 해당 정보의 암호화 또는 이에 상응하는 조치 라. 그 밖에 암호화 또는 이에 상응하는 기술을 이용한 보안조치 5. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 다음 각 목의 조치 가. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 나. 개인정보처리시스템에 대한 접속기록의 안전한 보관 다. 그 밖에 접속기록 보관 및 위조·변조 방지를 위하여 필요한 조치 6. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대해 컴퓨터 바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치 7. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 8. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치 ② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. ③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

3. 개정내용 해설

□ 개인정보처리자는 개인정보의 안전한 처리를 위하여 내부 관리계획을 수립·시행하고, 이에 대한 이행 실태를 점검 및 관리하여야 한다.

○ 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 세부적인 추진 방안을 포함한 내부 관리계획을 수립·시행하여야 하며,

○ 내부 관리계획에는 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항을 포함하여야 하고, 사업규모·개인정보 보유 수·업무성격 등에 따라 차등화하여 정기적으로 교육을 실시하여야 한다.

※ 내부 관리계획에는 법령 및「개인정보의 안전성 확보조치 기준」제4조에서 정하는 사항을 포함하여야 하며, 개인정보처리자 스스로 필요한 사항을 포함하여 정할 수 있음

※ 내부 관리계획의 수립·시행뿐만 아니라 '점검'에 대한 사항이 추가되었으므로, 내부 관리계획으로 수립한 사항을 이행하였는지를 연 1회 이상 점검해야 함

○ 또한, 개인정보처리자는 스스로의 환경을 고려하여 법 제31조 및 영 제32조에서 정하는 자격요건을 충족하는 자를 개인정보 보호책임자로 지정하여야 하며, 이에 관한 사항을 내부 관리계획에 포함하여야 한다.

※ 개인정보 보호책임자(CPO)와 「정보통신망법」 제45조의3에서 정하고 있는 정보보호 최고책임자(CISO)는 동일인으로 지정하거나 별도로 지정할 수 있으나, 「개인정보의 안전성 확보조치 기준」에 관하여 상호간의 업무를 명확히 분장하여 정할 필요가 있음

○ 다만, 내부 관리계획의 수립·시행 및 점검의 의무는 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

※ 「소상공인기본법」 제2조에 따른 소상공인과 개인, 단체만 해당하므로, 그 외의 개인정보처리자는 내부 관리계획을 수립·시행하여야 함

□ 개인정보처리자는 개인정보에 대한 접근 권한을 제한하기 위하여 필요한 접근권한의 관리, 인증수단의 적용 등 안전조치 기준을 수립・시행하여야 한다.

○ 개인정보처리시스템에 대한 접근 권한은 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 하며, 개인정보취급자의 업무가 변경*되는 경우에는 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

※ '업무의 변경'은 조직 내의 임직원 전보 또는 퇴직, 휴직 등 인사이동이 발생한 경우 및 조직의 변경 또는 업무 조정 등으로 인한 변경을 포함함

○ 또한, 개인정보처리자는 정당한 권한을 가진 개인정보취급자 또는 정보주체를 인증하기 위하여 스스로의 환경에 맞는 인증수단*을 안전하게 적용하고 관리해야 한다.

※ 인증수단 예시 : 비밀번호, 생체인증, 소셜 로그인, SMS 인증 등

○ 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유*가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

※ '정당한 사유'란 개인정보취급자의 계정은 원칙적으로 개별로 발급되어야 하나, 시스템이 제공하는 고정된 계정(root 등)과 같이 기술적으로 개별 발급이 불가능한 경우 등을 말함

□ 개인정보처리자는 개인정보처리시스템에 대한 침입을 탐지하고 차단하는 등 개인정보에 대한 접근을 통제하기 위한 조치를 하여야 한다.

○ 접근 통제를 위한 조치를 기술 중립적으로 개선하여 특정 시스템의 설치·운영 이외에 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위한 다양한 조치*를 할 수 있도록 개선하였다.

※ 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한, 접속한 인터넷 프로토콜(IP) 주소를 분석하여 개인정보 유출 시도를 탐지 및 대응 등

○ 또한, 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자* 수가 일일평균 100만명 이상인 경우에는 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단(망분리) 조치를 하여야 한다.

* 정보통신망법에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자

○ 다만, 클라우드 컴퓨팅서비스 이용이 확산됨에 따라 인터넷망 차단 조치의 기준을 명확히 하여, 클라우드 컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우*에는 해당 서비스에 대한 접속 외에 인터넷을 차단하는 조치를 할 수 있다.

* 클라우드 서버에 개인정보처리시스템을 설치·운영하는 경우(IaaS), 클라우드서비스가 제공하는 개인정보 처리 응용프로그램(고객관계관리, 인사회계 등)를 이용하는 경우(SaaS), 클라우드 사업자가 제공하는 DBMS 등을 이용하여 개인정보처리시스템을 구축·운영하는 경우(PaaS) 등

□ 개인정보처리자는 개인정보를 안전하게 전송, 저장하기 위하여 안전한 암호 알고리즘으로 암호화해야 하며, 기술환경 변화를 고려하여 이에 상응하는 조치도 가능하도록 개정하여 기술변화에 유연하게 대응할 수 있도록 개선하였다.

○ 일반규정과 특례규정 간 상이했던 정보통신망을 통한 전송 시 암호화 관련 규정을 통합하고, 사업자 영향 수준 등을 고려하여 저장 시 암호화 규정은 기존과 동일하게 유지하였다.

<table>
<tr><th colspan="2" rowspan="2">구분</th><th colspan="2">개인정보 보호법에 따른 암호화 대상 개인정보</th></tr>
<tr><th>이용자가 아닌 정보주체의 개인정보</th><th>이용자의 개인정보</th></tr>
<tr><td rowspan="2">정보통신망을 통한 송·수신 시</td><td>정보통신망</td><td colspan="2">인증정보(비밀번호, 생체인식정보 등)</td></tr>
<tr><td>인터넷망</td><td colspan="2">개인정보</td></tr>
<tr><td rowspan="5">저장 시</td><td rowspan="3">저장 위치 무관</td><td colspan="2">인증정보(비밀번호, 생체인식정보 등)
※ 단, 비밀번호는 일방향 암호화</td></tr>
<tr><td>-</td><td>신용카드번호, 계좌번호</td></tr>
<tr><td colspan="2">주민등록번호</td></tr>
<tr><td>인터넷구간, DMZ</td><td>고유식별정보
(주민등록번호 제외)</td><td rowspan="2">여권번호,
운전면허번호
외국인등록번호</td></tr>
<tr><td>내부망</td><td>고유식별정보
(주민등록번호 제외)
※ 영향평가 또는 위험도 분석을 통해 암호화 미적용 가능</td></tr>
<tr><td colspan="2">개인정보취급자 컴퓨터, 모바일기기, 보조저장매체 등에 저장 시</td><td>고유식별정보, 생체인식정보</td><td>개인정보</td></tr>
</table>

□ 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보취급자의 접속기록을 보관·관리하고 월 1회 이상 점검하여야 하며,

○ 개인정보취급자의 접속기록은 1년 이상 보관·관리하여야 하고, 다음에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

< 접속기록의 2년 보관·관리 대상 >

- 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
- 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
- 개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

○ 또한, 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관·관리하여야 하며, 별도의 물리적인 저장장치에 보관하는 방법 외에 다양한 방법을 활용할 수 있다.

□ 개인정보처리자는 악성프로그램 등을 통해 개인정보가 위·변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 보안 프로그램을 설치·운영하여야 한다.

○ 보안 프로그램은 그 목적과 기능에 따라 다양한 종류의 제품이 있으므로 개인정보처리자는 스스로의 환경에 맞게 설치·운영이 가능하며, 개인정보처리자는 설치한 보안 프로그램을 일 1회 이상 업데이트하는 등 보안 프로그램을 최신의 상태로 유지하여야 한다.

○ 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유*가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

* '정당한 사유'란 보안 업데이트 적용 시 개인정보처리시스템의 안정성 점검이 필요한 경우 등을 말함

□ 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두는 경우 출입통제 절차를 수립·운영하여야 하며,

○ 출입 요청 및 승인, 출입 기록 작성, 출입 기록 관리 등 물리적 보관 장소에 대한 출입통제 절차를 수립하고 운영해야 한다.

○ 또한, 개인정보가 포함된 서류, 보조저장매체 등은 잠금장치가 있는 캐비닛 등 안전한 장소에 보관하고 개인정보가 유출되지 않도록 반출·입 통제를 위한 보안대책을 마련하여야 한다.

4. 개인정보처리자 유의사항

□ 시행령 제30조 및 「개인정보의 안전성 확보조치 기준」에서의 내용은 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준으로, 개인정보처리자는 스스로 환경에 맞는 조치를 하여야 한다.

◈ 자세한 사항은 개인정보의 안전조치 관련 해설서 참조
1. 개인정보의 안전성 확보 조치 기준 해설서
2. 개인정보의 암호화 조치 안내서
3. 개인정보 위험도 분석 기준 및 해설서

5. 제재 규정

위반행위	제재 내용
안전성 확보에 필요한 조치를 하지 아니한 자 (제29조 위반)	3천만원 이하의 과태료 (제75조제2항제5호)
개인정보처리자가 처리하는 개인정보가 분실・도난・유출・위조・변조・훼손된 경우. 다만, 개인정보가 분실・도난・유출・위조・변조・훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.	과징금 부과 (제64조의2제1항제9호)

6. 질의 응답

□ 내부 임직원들의 개인정보를 처리하기 위한 시스템도 개인정보처리시스템에 해당하는지?

⇨ 내부 임직원들의 개인정보를 저장한 데이터베이스(DB)에 접근하여 조회(검색)하는 것은 개인정보 '처리'에 해당하며, 데이터베이스(DB)에 접근하여 조회하는 시스템은 개인정보처리시스템에 해당함

⇨ 보안 솔루션, 네트워크 관리 시스템 등에서 계정 관리, 알림 통지 등을 위해 임직원의 이름, 연락처, 이메일 등의 개인정보를 처리하는 경우 개인정보처리시스템에 해당함

□ 개정된 「개인정보의 안전성 확보조치 기준」 조항별 시행 시기는?

⇨ 안전조치 의무가 강화되는 일부 조항의 경우 '24.9.15.부터 적용됨

⇨ 다만, 일반규정에서 특례규정으로 확대되는 조항은 특례규정을 적용받던 정보통신서비스 제공자에 유예기간이 적용되고, 반대로 특례규정이 일반규정으로 확대되는 조항은 일반규정을 적용받던 개인정보처리자에 유예기간이 적용됨

※ 자세한 사항은 개정「개인정보의 안전성 확보조치 기준」부칙 참조

□ 접근 권한의 부여, 변경, 말소 등을 수기로 기록해도 되는지?

⇨ 영 제30조 및「개인정보의 안전성 확보조치 기준」제5조에서는 접근 권한의 부여, 변경 또는 말소에 대한 내역을 기록하도록 규정하고 있을 뿐 구체적인 방법에 대해서는 안내하고 있지 않음

⇨ 따라서 해당 기록을 시스템을 통해 DB에 기록하는 방법, 내부 수기 결재 등 방법을 통하여 기록을 할 수 있음

□ 비밀번호 작성규칙을 개인정보처리자가 임의로 정해도 되는지?

⇨ 개인정보처리자는 정당한 권한을 가진 자인지를 인증하기 위해 비밀번호, 생체인증 등 다양한 인증수단 도입할 수 있음

⇨ 개인정보취급자의 비밀번호 작성규칙(예: 문자열 조합, 변경주기 등)에 관한 종전 기준은 삭제되었으므로, 개인정보를 처리하는 방법 및 환경 등을 고려하여 정당한 접속권한을 가지지 않은 자가 추측하거나 접속을 시도하기 어렵게 비밀번호 작성규칙을 수립하여 운영하여야 함

□ 침입 탐지 및 유출 탐지 기능을 갖춘 접근통제 장치만 설치해도 법령 및 하위 고시에서 정한 사항을 충족하는지?

⇨ 단순히 방화벽 등 정보보호 솔루션을 구매 및 설치하는 것만으로는 영 제30조 및「개인정보의 안전성 확보조치 기준」에서 규정한 접근통제 조치를 이행하였다고 보기 어려움

⇨ 신규 위협에 대응할 수 있도록 지속적으로 정책설정의 지속적인 업데이트 적용 및 운영·관리, 이상행위 대응, 로그분석 등의 방법으로 체계적으로 운영·관리해야 함

□ 개인정보 출력시 마스킹을 하지 않아도 되는지?

⇨「개인정보의 안전성 확보조치 기준」제12조 제1항에서 개인정보의 출력시 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하도록 규정하고 있음. 따라서, 출력 항목을 최소화하는 방법으로 마스킹 기법을 활용할 수 있음

□ 이용자의 개인정보와 이용자가 아닌 정보주체의 개인정보는 어떻게 구분되는지?

⇨ 이용자의 개인정보는 ①정보통신서비스 제공자가 제공하는 ②정보통신서비스를 이용하는 자의 개인정보를 의미함

⇨ 따라서 정보통신서비스 제공자가 아닌 공공기관 및 오프라인 사업자 등이 수집·이용하는 정보주체의 개인정보는 이용자가 아닌 정보주체의 개인정보에 해당함

⇨ 또한 정보통신서비스 제공자라도 임직원 등 개인정보취급자의 개인정보, 오프라인으로 수집하여 저장·관리하는 고객의 개인정보는 이용자가 아닌 정보주체의 개인정보에 해당함

□ 정보통신망과 인터넷망은 어떻게 다른지?

⇨ 정보통신망은 내부망과 외부망(인터넷망 등)을 포함한 모든 통신망을 의미하며, 인터넷망은 정보통신망 중에서 인터넷 서비스에 연결된 통신망만을 의미함

□ 외부에서 이용자의 개인정보를 처리하는 개인정보처리시스템에 접속 시 VPN을 적용하고 있는 경우에도 안전한 인증수단을 적용해야 하는지?

⇨ 정보통신망을 통해 외부에서 이용자의 개인정보를 처리하는 개인정보처리시스템에 접속하려는 경우에는 안전한 인증수단을 적용하여야 함

⇨ 다만, VPN 접속 시 안전한 인증수단을 적용하고 있는 경우 해당 VPN을 통해 접속하는 개인정보처리시스템에 대해 안전한 인증수단을 적용한 것으로 볼 수 있음

□ 인터넷망 차단(망분리) 조치 의무가 일반 개인정보처리자에게도 확대되는지?

⇨ 인터넷망 차단 조치는 이용자 수가 일일평균 100만명 이상인 개인정보처리자에만 해당되며, 이용자는 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 의미하므로 이용자의 개인정보를 처리하지 않는 개인정보처리자에는 인터넷망 차단 조치 의무가 적용되지 않음

□ 개정 시행령에서 이용자 수가 100만명 이상인 경우만 인터넷망 차단 조치를 하도록 되어 있는데 매출액 100억원 이상인 경우 망분리 적용 의무가 사라지는지?

⇨ 인터넷망 차단 조치를 해야 하는 개인정보처리자의 기준에서 종전의 매출액 100억원 이상 기준은 삭제되었으므로 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이 아니라면 인터넷망 차단 조치 의무 대상이 아님

□ 인터넷망 차단 조치에서 개인정보가 저장·관리되고 있는 이용자의 수 기준이 개인정보처리자가 기준인지, 개인정보처리시스템이 기준인지?

⇨ 인터넷망 차단 조치는 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 적용됨

⇨ 이는 개인정보처리자가 일일평균 저장·관리하고 있는 이용자 수가 기준으로, 개인정보처리자가 개인정보처리시스템 별로 나눠서 저장·관리하더라도 합산하여 산정하여야 하며 이에는 분리보관하고 있는 휴면회원 등의 이용자 수도 포함됨

□ 내부망에 저장하는 주민등록번호는 영향평가나 위험도 분석을 통해 암호화하지 않고 보유할 수 있는지?

⇨ 주민등록번호는 법 제24조의2, 동법 시행령 제21조의2에 따라 "개인정보 영향평가"나 "암호화 미적용시 위험도 분석"의 결과에 관계없이 암호화하여야 함

□ 비정형데이터도 암호화하여야 하는지?

⇨ 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화)에서는 비정형데이터 및 정형데이터에 따라 세부적인 기준을 정하고 있지 않음. 따라서, 비정형 데이터로 저장된 경우라도 암호화 대상이 포함되는 경우 암호화하여야 함

□ 공공기관도 모든 개인정보를 인터넷망에서 전송하는 경우 암호화해야 하는지?

⇨ 종전에는 고유식별정보·비밀번호·생체인식정보만 암호화 대상이었으나 고시 개정에 따라 모든 개인정보를 인터넷망 구간으로 전송하는 경우 암호화하여야 함

□ 기존에는 개인정보취급자에 대한 접속기록을 보관하고 관리하도록 의무화되어 있었는데, 이제는 이용자의 접속기록도 보관하고 관리해야 하는지?

⇨ 개인정보처리시스템에 접속한 자의 접속기록을 보관·관리하도록 한 「개인정보의 안전성 확보조치 기준」 행정예고안('23.7월)의 제8조 제1항은 개정 고시에서 삭제되었으므로 개인정보 보호법 상 이용자의 접속기록 보관 의무는 없음

□ 개인정보 처리 목적을 달성하여 파기하는 경우라도 개인정보취급자의 접속기록은 보관해야 하는지?

⇨ 개인정보취급자의 접속기록을 보관하도록 하는 것은 개인정보를 처리하는 개인정보취급자의 업무수행과 관련하여 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하고 적절한 조치를 하는 등의 책임 추적성 확보를 위한 취지이므로, 영 제30조 및 「개인정보의 안전성 확보조치 기준」 제8조에서 정한 사항에 따른 기간 동안 접속기록을 보관해야 함

참고 개인정보의 안전성 확보조치 기준('23.9.22. 시행)

제1장 총칙

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제29조와 같은 법 시행령(이하 "영"이라 한다) 제16조제2항, 제30조 및 제30조의2에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
2. "이용자"란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
3. "접속기록"이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
4. "정보통신망"이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
5. "P2P(Peer to Peer)"란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
6. "공유설정"이란 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
7. "모바일 기기"란 무선망을 이용할 수 있는 스마트폰, 태블릿 컴퓨터 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
8. "비밀번호"란 정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
9. "생체정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
10. "생체인식정보"란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
11. "인증정보"란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보를 말한다.
12. "내부망"이란 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
13. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
14. "보조저장매체"란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 연결·분리할 수 있는 저장매체를 말한다.

제2장 개인정보의 안전성 확보조치

제3조(안전조치의 적용 원칙) 개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용하여야 한다.

제4조(내부 관리계획의 수립·시행 및 점검) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

1. 개인정보 보호 조직의 구성 및 운영에 관한 사항
2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
7. 개인정보의 암호화 조치에 관한 사항
8. 접속기록 보관 및 점검에 관한 사항
9. 악성프로그램 등 방지에 관한 사항
10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
11. 물리적 안전조치에 관한 사항
12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
13. 위험 분석 및 관리에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
16. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검·관리 하여야 한다.

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.

② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.

⑥ 개인정보처리자는 정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.

③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.

⑤ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치를 하여야 한다. 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 한다.

제7조(개인정보의 암호화) ① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우

2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)

가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

나. 암호화 미적용시 위험도 분석에 따른 결과

④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
3. 개인정보처리자로서 「전기통신사업법」 제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

제9조(악성프로그램 등 방지) ① 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지
2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

제10조(물리적 안전조치) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제11조(재해·재난 대비 안전조치) 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중

견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다.

1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검
2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련

제12조(출력·복사시 안전조치) ① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.

② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제

③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.

제3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치

제14조(공공시스템운영기관의 안전조치 기준 적용) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템 중에서 개인정보보호위원회(이하 "보호위원회"라 한다)가 지정하는 개인정보처리시스템(이하 "공공시스템"이라 한다)을 운영하는 공공기관(이하 "공공시스템운영기관"이라 한다)은 제2장의 개인정보의 안전성 확보 조치 외에 이 장의 조치를 하여야 한다.

1. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 한 단일접속 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
   가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
   나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
   다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템
2. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템으로서 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우
3. 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 개별 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
   가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
   나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
   다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템
   라. 총 사업비가 100억원 이상인 시스템

② 제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템에 대하여는 공공시스템으로 지정하지 않을 수 있다.

1. 체계적인 개인정보 검색이 어려운 경우
2. 내부적 업무처리만을 위하여 사용되는 경우
3. 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우로서 보호위원회가 인정하는 경우

제15조(공공시스템운영기관의 내부 관리계획의 수립·시행) 공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립하여야 한다.

1. 영 제30조의2제4항에 따른 관리책임자(이하 "관리책임자"라 한다)의 지정에 관한 사항
2. 관리책임자의 역할 및 책임에 관한 사항
3. 제4조제1항제3호에 관한 사항 중 개인정보취급자의 역할 및 책임에 관한 사항
4. 제4조제1항제4호부터 제6호까지 및 제8호에 관한 사항
5. 제16조 및 제17조에 관한 사항

제16조(공공시스템운영기관의 접근 권한의 관리) ① 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다.

② 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 제5조제4항에 따른 계정을 발급해서는 안 된다. 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 그러하지 아니하며, 그 사유를 제5조제3항에 따른 내역에 포함하여야 한다.

③ 공공시스템운영기관은 제5조제4항에 따른 계정을 발급할 때에는 개인정보 보호 교육을 실시하고, 보안 서약을 받아야 한다.

④ 공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근 권한이 부여·관리되고 있는지 확인하기 위하여 제5조제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1회 이상 점검하여야 한다.

⑤ 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 "공공시스템이용기관"이라 한다)은 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여·관리를 직접하는 경우 제2항부터 제4항까지의 조치를 하여야 한다.

제17조(공공시스템운영기관의 접속기록의 보관 및 점검) ① 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용·남용 시도를 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치를 하여야 한다.

② 공공시스템운영기관은 공공시스템이용기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.

제18조(재검토 기한) 개인정보보호위원회는 「행정규제기본법」 제8조 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 9월 15일을 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-6호, 2023. 9. 22.>

이 고시는 발령한 날부터 시행한다. 다만, 다음 각 호의 개정규정은 각 호의 구분에 해당하는 개인정보처리자에 대해서는 2024년 9월 15일부터 시행한다.

1. 제5조제6항, 제7조제6항, 제8조제2항, 제11조의 개정규정 : 종전의 「(개인정보보호위원회) 개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회고시 제2021-3호) 적용대상인 개인정보처리자
2. 제7조제4항, 제12조제2항의 개정규정 및 제5조제6항 중 정보주체에 관한 개정규정 : 종전의 「(개인정보보호위원회) 개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시 제2021-2호) 적용대상인 개인정보처리자
3. 제14조부터 제17조까지의 개정규정 : 공공시스템운영기관과 공공시스템이용기관

2 공공시스템운영기관 등의 안전성 확보 조치 (영 제30조의2)

1. 개정 개요

□ 최근 공공시스템에서의 개인정보 유출로 인해 국민의 2차 피해*가 발생하고 있어 이를 막기 위해 대규모 개인정보를 처리하는 공공시스템을 운영하는 공공기관이 추가로 준수해야 하는 안전성 확보 조치를 신설하였다.

* n번방 사건('19년), 송파 살인사건('21.12월), 신당동 역무원 살인사건('22.9월) 등

2. 법령

법률	**제29조(안전조치의무)** 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
시행령	**제30조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등)** ① 개인정보의 처리 규모, 접근 권한을 부여받은 개인정보취급자의 수 등 보호위원회가 고시하는 기준에 해당하는 개인정보처리시스템(이하 이 조에서 "공공시스템"이라 한다)을 운영하는 공공기관(이하 이 조에서 "공공시스템운영기관"이라 한다)은 법 제29조에 따라 이 영 제30조의 안전성 확보 조치 외에 다음 각 호의 조치를 하여야 한다. 1. 제30조제1항제1호에 따른 내부 관리계획에 공공시스템별로 작성한 안전성 확보 조치를 포함할 것 2. 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 "공공시스템이용기관"이라 한다)이 정당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치 3. 개인정보에 대한 불법적인 접근 및 침해사고 방지를 위한 공공시스템 접속기록의 저장·분석, 점검·관리 등의 조치 ② 공공시스템운영기관 및 공공시스템이용기관은 정당한 권한 없이 또는 허용된 권한을 초과하여 개인정보에 접근한 사실이 확인된 경우에는 지체 없이 정보주체에게 해당 사실과 피해 예방 등을 위해 필요한 사항을 통지해야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 본문에 따른 통지를 한 것으로 본다. 1. 법 제34조제1항에 따라 정보주체에게 개인정보의 분실·도난·유출에 대하여 통지한 경우 2. 다른 법령에 따라 정보주체에게 개인정보에 접근한 내역과 피해 예방을 위해 필요한 사항을 통지한 경우 ③ 공공시스템운영기관(공공시스템을 개발하여 배포하는 공공기관이 따로 있는 경우에는 그 공공기관을 포함한다. 이하 이 조에서 같다)은 해당 공공시스템의 규모와 특성, 해당 공공시스템이용기관의 수 등을 고려하여 개인정보의 안전한 관리를 위해 필요한 업무를 전담하는 부서를 지정하여 운영하거나 전담인력을 배치해야 한다.

	④ 공공시스템운영기관은 공공시스템 각각에 대하여 해당 공공시스템을 총괄하여 관리하는 부서의 장을 관리책임자로 지정하여야 한다. 다만, 해당 공공시스템을 총괄하여 관리하는 부서가 없을 때에는 업무 관련성 및 수행능력 등을 고려하여 해당 공공시스템운영기관의 관련 부서의 장 중에서 관리책임자를 지정하여야 한다. ⑤ 공공시스템운영기관은 공공시스템에 대한 안전성 확보 조치 이행상황을 점검하고 개선하기 위하여 다음 각 호의 기관으로 구성된 공공시스템 협의회를 설치·운영하여야 한다. 다만, 하나의 공공기관이 다수의 공공시스템을 운영하는 경우에는 기관, 분야, 시스템 등의 특성을 고려하여 공공시스템 협의회를 통합하여 설치·운영할 수 있다. 1. 공공시스템운영기관 2. 공공시스템의 운영을 위탁하는 경우의 해당 수탁자 3. 공공시스템운영기관이 공공시스템의 안전성 확보 조치의 개선 및 점검을 위하여 필요하다고 인정하는 공공시스템이용기관 ⑥ 보호위원회는 공공시스템운영기관이 안전성 확보 조치를 이행하는데 필요한 지원을 할 수 있다. ⑦ 제1항부터 제6항까지에서 규정한 사항 외에 공공시스템운영기관의 개인정보 안전성 확보 조치에 필요한 사항은 보호위원회가 정하여 고시한다.

3. 개정내용 해설

□ 시행령 제30조의2의 공공시스템이란 개인정보 보유량, 취급자 수 등을 고려하여 보호위원회가 지정하는 집중관리시스템을 말하며,

○ 보호위원회는 「공공부문 개인정보 유출 방지대책('22.7월)」과 「공공부문 집중관리시스템 개인정보 안전조치 강화계획('23.4월)」을 수립하면서 선정된 집중관리시스템 1,515개(126종)를 지정하였고, 단계적으로 확대 지정할 예정이다.

* 수범 대상자는 공공시스템 개발·운영기관과 이용기관임. 이용기관에는 공공시스템에 대한 접근권한을 부여 받아 이를 이용하는 공공기관과 배포된 공공시스템 패키지를 설치·이용하는 공공기관을 포함함

□ 시행령 제30조의2 공공시스템 안전조치 특례의 주요 내용은 다음과 같다.

○ 첫째, 공공시스템 협의회* 설치·운영(제5항), 공공시스템별 책임자 지정(제4항) 및 안전성 확보 조치 방안**을 포함한 내부 관리계획 수립(제1항제1호) 등 공공시스템에 대한 통합적 관리체계를 구축하여야 한다.

* 공공시스템 협의회는 시스템별로 설치하는 것이 원칙이나, 운영중인 공공시스템 개수나 공공시스템별 특성을 고려하여 기관별 또는 유형별로 통합 설치 가능

** 접근권한, 접속기록, 암호화 등 내부관리계획 각 조항 아래 공공시스템별 안전조치 방안을 규정하여야 함. 다만, 공공시스템 운영기관의 사정에 따라 공공시스템을 유형별로 묶어 정하거나 공공시스템별 안전조치 방안을 별지로 수립하는 것도 가능함

○ 둘째, 취급자의 계정 발급·말소를 인사정보와 연계*하거나, 공무원이 아닌 자에 대한 예외적인 발급절차** 도입 등 접근권한의 안전한 관리를 위해 필요한 조치를 하여야 한다. (제1항제2호)

* 취급자에 대한 인사정보(전자인사시스템, LDAP, 산하 공공기관 자체 인사정보 등)와 연계하여 인사정보에 포함되어 있는 취급자에 대해서만 접근권한을 부여하거나, 인사이동(전보, 휴직, 퇴직 등)으로 해당 공공시스템과 관련한 업무를 수행하지 않을 때 자동으로 계정을 말소시키는 것을 의미함

** 일부 공공시스템은 공무원이 아닌 민간인도 이용하는 경우가 있으며, 이 경우 민간인이 소속된 기관의 장이 예외적 계정발급 사유를 소명하여야 하고, 계정발급 전 해당 민간인에게 개인정보 보호 교육을 실시해야 하며, 보안서약서를 징구해야 함(공공시스템 내에서 전자적 방법으로도 이행 가능)

○ 셋째, 공공시스템 개발·운영기관 외에 이용기관도 소관 취급자의 접속기록을 점검* 해야 하고, 정상적이지 않은 접근행위는 탐지·차단**하는 등 접속기록의 저장·분석 및 점검·관리 등의 조치를 하여야 한다. (제1항제3호)

* 접속기록은 고시 제2조제19조에서 정한 접속지 정보 등 5개 항목을 모두 생성· 보관하여야 하며, 개발·운영기관만 분석·점검하는 것이 아니라 이용기관도 소속 취급자의 접속기록을 점검·분석·관리할 수 있어야 함

** 비정상 접근행위는 휴일·근무시간 외 시스템 접속 및 개인정보 열람·저장이나, 대량의 개인정보를 열람·저장 하는 등의 행위로 공공시스템이 처리하는 업무의 특성 및 취급자의 근무형태 등을 고려하여 미리 설정하여야 함. 이러한 기준에 해당하는 접속기록은 별도로 보관하고 해당 취급자가 사전에 소속 부서장에게 승인을 받거나 사후에 소명하도록 점검·관리되어야 함

○ 넷째, 공공시스템운영기관 및 공공시스템이용기관은 정당한 권한 없이 또는 허용된 권한을 초과하여 개인정보에 접근한 사실이 확인되는 경우에는 지체 없이 정보주체에게 해당 사실과 피해 예방 등을 위해 필요한 사항을 통지해야 한다. (제2항)

○ 다섯째, 공공시스템 운영기관은 소관 공공시스템의 규모와 특성 취급자 수 등을 고려하여 개인정보를 안전하게 관리할 수 있도록 전담 부서를 지정·운영하거나 전담 인력을 배치해야 한다. (제3항)

4. 개인정보처리자 유의사항

□ 공공시스템운영기관의 예산 협의, 시스템 고도화 등 준비기간을 고려하여, 계도 기간을 두고 시행 시기를 2024년 9월 15일부터로 시행령 부칙에 정하였다.

□ 공공시스템 지정은 개인정보 보유량, 취급자 수 등을 고려하여 보호위원회가 지정하고, 그 결과를 보호위원회 홈페이지(www.pipc.go.kr)에 공지할 계획이며, 단계적으로 공공시스템 지정을 확대해 나갈 예정이다.

5. 제재 규정

위반행위	제재 내용
안전성 확보에 필요한 조치를 하지 아니한 자 (제29조 위반)	3천만원 이하의 과태료 (제75조제2항제5호)
개인정보처리자가 처리하는 개인정보가 분실・도난・유출・위조・변조・훼손된 경우. 다만, 개인정보가 분실・도난・유출・위조・변조・훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.	과징금 부과 (제64조의2제1항제9호)

6. 질의 응답

□ 영 제30조의2는 모든 공공시스템운영기관에 적용되는지?

⇨ 적용 대상은 공공시스템운영기관 중에서 개인정보 보유량, 취급자 수 등을 고려하여 보호위원회가 지정하는 공공시스템운영기관 및 이용기관에 한정하고 있음

□ 공공시스템 운영기관이 영 제30조의2를 위반하면 어떻게 되는지?

⇨ 영 제30조의2를 위반하는 경우 법 제29조에 따른 안전조치 의무 위반이 되며, 법 제75조제2항에 따라 3,000만원 이하의 과태료 부과 대상임

□ 특례 이행에는 다른 기관과 협의나 예산을 수반한 시스템 고도화 등 많은 시간이 소요될 것인데, 언제부터 시행되는지?

⇨ 원칙적으로, 영 제30조의2의 신설규정은 2024년 9월 15일부터 시행 예정임

□ 내부 관리계획에 포함되어야 하는 안전성 확보조치 기준은 무엇인지?

⇨ 시행령에 신설된 제30조의2에 따라 공공시스템운영기관 등에 부여되는 협의회 설치·운영, 시스템별 책임자 지정·운영, 접근권한 부여·관리 및 접속기록 관리·점검 등 강화된 안전조치 의무 이행 방향을 구체적으로 수립하라는 의미임

6 개인정보 유출등의 통지 및 신고(법 제34조)

1. 개정 개요

□ 그동안 일반규정과 특례규정의 유출 통지·신고 규정이 달라 온·오프라인 여부에 따라 동일 위반행위에 대하여 다른 요건을 적용하여 현장에서의 혼란을 야기함

○ 이에 따라, 법 개정을 통해 온·오프라인과 관계없이 개인정보 유출등이 되었음을 알게 된 경우에는 동일한 통지 및 신고 기준을 적용하도록 정비하였다.

※ 일반 개인정보처리자와 정보통신서비스 제공자 모두에 해당하는 사업자의 경우, 각각 다른 방식으로 유출 통지·신고를 해야 하는 문제가 발생

2. 법령

법률	**제34조(개인정보 유출 등의 통지·신고)** ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 "유출등"이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. 1. 유출등이 된 개인정보의 항목 2. 유출등이 된 시점과 그 경위 3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 4. 개인정보처리자의 대응조치 및 피해 구제절차 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 ② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다. ③ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다. ④ 제1항에 따른 유출등의 통지 및 제3항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.
시행령	**제39조(개인정보 유출 등의 통지)** ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조 및 제40조에서 "유출등"이라 한다)되었음을 알게 되었을 때에는 서면등의 방법으로 72시간 이내에 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다. 1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우 2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우

	② 제1항에도 불구하고 개인정보처리자는 같은 항에 따른 통지를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 통지해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지해야 한다. ③ 제1항 및 제2항에도 불구하고 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 법 제34조제1항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다. **제40조(개인정보 유출 등의 신고)** ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 법 제34조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 같은 조 제3항 전단에 따른 전문기관에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다. 1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우 2. 민감정보 또는 고유식별정보가 유출등이 된 경우 3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우 ② 제1항에도 불구하고 개인정보처리자는 제1항에 따른 신고를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다. ③ 법 제34조제3항 전단 및 후단에서 "대통령령으로 정하는 전문기관"이란 각각 한국인터넷진흥원을 말한다.

3. 개정내용 해설

□ 개인정보 유출 통지의 경우 시행령 제39조에서 개인정보가 유출되었음을 알게 되었을 때에는 72시간 이내에 정보주체에게 알리도록 기준을 일원화하였다.

○ 다만, 일정한 사유에 해당하는 경우*에는 해당 사유 해소 후 통지가 가능하도록 보완하였다.

* ① 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우, ② 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우 등

○ 아울러 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 인터넷 홈페이지에 30일 이상 게시하는 것으로 통지를 갈음하는 것으로 규정을 일원화하였다.

□ 유출 신고의 경우 시행령 제40조에서 ①1천명 이상 유출되었거나, ②민감정보·고유식별정보가 1건 이상 유출 또는 ③외부로부터의 불법적인 접근(해킹)에 의해 1건 이상 유출되었음을 알게 되었을 때에는 72시간 이내에 신고하도록 규정을 일원화하였다.

※ 규모만 고려하도록 한 종전법과 달리 개정법은 개인정보 유형, 유출 경로·규모 등을 고려하도록 명시한 점을 고려하여 시행령에 구체화

○ 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유 해소 후 신고가 가능하도록 하였으며,

○ 종전에는 예외 없이 신고해야 했으나, 현행법에는 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮은 경우에는 신고를 하지 않을 수 있도록 예외 규정을 신설하였다.

4. 개인정보처리자 유의사항

□ 개정법 제34조 개인정보 유출 등의 통지·신고에 관한 규정은 2023년 9월 15일 법 시행 이후 개인정보가 분실·도난·유출되었음을 알게 된 경우부터 적용한다.

5. 제재 규정

위반행위	제재 내용
제34조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자	3천만원 이하의 과태료 (제75조제2항제17호)
제34조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하지 아니한 자	3천만원 이하의 과태료 (제75조제2항제18호)

6. 질의 응답

□ 통지·신고 기한(72시간) 예외 사유는?

⇨ 개인정보 유출과 관련하여 수사기관의 비공개 요청이 있는 경우, 물리적·기술적·관리적인 사유로 통지가 불가능한 경우를 예로 들 수 있음

□ 개인정보처리자는 개인정보가 유출 등 되었음을 알게 되었을 때에는 72시간 이내에 통지하여야 하는데, 통지 기한 산정 시 공휴일 등 근무일 외의 날은 제외해도 되는지?

⇨ 개인정보의 유출 등 통지는 정보주체의 권익 침해 가능성 등을 최소화하기 위한 조치임 따라서 개인정보처리자는 개인정보 유출 등을 알게된 이상, 그 사이에 공휴일 등 근무일 외의 날이 포함되어 있다 하더라도 이를 별도로 고려하지 않고 그 시점으로부터 72시간 이내에 통지하여야 함

7 개인정보 분쟁조정제도 개선(법 제40~47조, 제50조의2)

1. 개정 개요

□ 국민의 개인정보 보호 인식이 높아져 개인정보에 대한 분쟁조정 신청건수*는 지속적으로 증가하고 있으며, 분쟁조정 신청이 접수되면 공공기관은 반드시 분쟁조정에 응하여야 하므로 정보주체의 피해구제가 가능하였으나,

○ 민간 기업은 분쟁조정에 응할 의무가 없어 분쟁조정에 응하지 않는 경우가 있어 실효적·적극적 분쟁해결에 한계**가 있었다.

* 연도별 신청건수: ('19) 352건 →('20) 431건 → ('21) 870건→ ('22년) 976건

** 피신청인('22년): 민간부문(846건, 86.7%) > 공공부문(130건, 13.3%)

□ 이에 분쟁조정 의무 참여의 전면 확대, 조정안에 대한 수락 여부를 알리지 않은 경우 수락 간주 도입, 사실관계 확인을 위한 사실조사권 신설 등 개인정보 분쟁조정제도를 개선하여 국민의 개인정보에 대한 권리보장과 피해구제를 강화하였다.

2. 법령

법률	**제40조(설치 및 구성)** ② 분쟁조정위원회는 위원장 1명을 포함한 30명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다. **제43조(조정의 신청 등)** ③ 개인정보처리자가 제2항에 따른 분쟁조정의 통지를 받은 경우에는 특별한 사유가 없으면 분쟁조정에 응하여야 한다. **제45조(자료의 요청 및 사실조사 등)** ② 분쟁조정위원회는 분쟁의 조정을 위하여 사실 확인이 필요한 경우에는 분쟁조정위원회의 위원 또는 대통령령으로 정하는 사무기구의 소속 공무원으로 하여금 사건과 관련된 장소에 출입하여 관련 자료를 조사하거나 열람하게 할 수 있다. 이 경우 분쟁당사자는 해당 조사·열람을 거부할 정당한 사유가 있을 때에는 그 사유를 소명하고 조사·열람에 따르지 아니할 수 있다. ③ 제2항에 따른 조사·열람을 하는 위원 또는 공무원은 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다. ④ 분쟁조정위원회는 분쟁의 조정을 위하여 필요하다고 인정하면 관계 기관 등에 자료 또는 의견의 제출 등 필요한 협조를 요청할 수 있다. ⑤ 분쟁조정위원회는 필요하다고 인정하면 분쟁당사자나 참고인을 위원회에 출석하도록 하여 그 의견을 들을 수 있다. **제47조(분쟁의 조정)** ③ 제2항에 따라 조정안을 제시받은 당사자가 제시받은 날부터 15일 이내에 수락 여부를 알리지 아니하면 조정을 수락한 것으로 본다. ④ 당사자가 조정내용을 수락한 경우(제3항에 따라 수락한 것으로 보는 경우를 포함한다) 분쟁조정위원회는 조정서를 작성하고, 분쟁조정위원회의 위원장과 각 당사자가 기명날인 또는 서명을 한 후 조정서 정본을 지체 없이 각 당사자 또는 그 대리인에게 송달하여야 한다. 다만, 제3항에 따라 수락한 것으로 보는 경우에는 각 당사자의 기명날인 및 서명을 생략할 수 있다.

	제50조의2(개선의견의 통보) 분쟁조정위원회는 소관 업무 수행과 관련하여 개인정보 보호 및 정보주체의 권리 보호를 위한 개선의견을 보호위원회 및 관계 중앙행정기관의 장에게 통보할 수 있다.
시행령	**제49조의2(분쟁조정 전문위원회)** ① 분쟁조정위원회는 개인정보에 관한 분쟁의 조정과 관련된 사항의 전문적인 검토를 위하여 분쟁조정위원회에 분야별 전문위원회(이하 "분쟁조정전문위원회"라 한다)를 둘 수 있다. ② 분쟁조정전문위원회는 위원장 1명을 포함한 10명 이내의 위원으로 구성한다. ③ 분쟁조정전문위원회 위원은 다음 각 호의 사람 중에서 분쟁조정위원회 위원장이 임명하거나 위촉하고, 분쟁조정전문위원회 위원장은 분쟁조정전문위원회 위원 중에서 분쟁조정위원회 위원장이 지명한다. 1. 분쟁조정위원회 위원 2. 개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원 3. 대학에서 개인정보 보호 분야의 조교수 이상으로 재직하고 있거나 재직하였던 사람 4. 공인된 연구기관에서 개인정보 보호 관련 분야의 5년 이상 연구경력이 있는 사람 5. 변호사 자격을 취득한 후 개인정보 보호 관련 분야에 1년 이상 경력이 있는 사람 6. 그 밖에 개인정보 보호 및 분쟁의 조정과 관련하여 전문지식과 경험이 풍부한 사람 ④ 제1항부터 제3항까지에서 규정한 사항 외에 분쟁조정전문위원회의 구성 및 운영 등에 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회 위원장이 정한다. **제51조의2(조정 불응 의사의 통지)** 법 제43조제3항에 따른 특별한 사유가 있어 분쟁조정에 응하지 않으려는 개인정보처리자는 법 제43조제2항에 따른 분쟁조정의 통지를 받은 날부터 10일 이내에 그 사유를 명시하여 분쟁조정 불응 의사를 분쟁조정위원회에 알려야 한다. **제51조의3(분쟁조정위원회의 사무기구 및 조사·열람 등)** ① 법 제45조제2항 전단에서 "대통령령으로 정하는 사무기구"란 제50조제1항에 따라 분쟁조정에 필요한 사무처리를 담당하는 보호위원회의 사무기구를 말한다. ② 분쟁조정위원회는 법 제45조제2항에 따라 조사·열람을 하려는 경우에는 그 7일 전까지 조사·열람 대상자에게 다음 각 호의 사항을 문서로 알려야 한다. 다만, 조사·열람 목적을 침해할 우려가 있는 경우에는 미리 알리지 않을 수 있다. 1. 조사·열람의 목적 2. 조사·열람의 기간과 장소 3. 조사·열람을 하는 사람의 직위와 성명 4. 조사.열람의 범위와 내용 5. 정당한 사유가 있는 경우 조사·열람을 거부할 수 있다는 사실 6. 정당한 사유 없이 조사·열람을 거부·방해 또는 기피할 경우 불이익의 내용 7. 그 밖에 분쟁조정을 위한 조사·열람에 필요한 사항 ③ 분쟁조정위원회는 법 제45조제2항에 따라 조사·열람을 할 때에는 분쟁당사자 또는 분쟁당사자가 지명하는 자가 입회하거나 의견을 진술하도록 요청할 수 있다. ④ 분쟁조정위원회는 법 제45조제5항에 따라 의견을 들으려면 회의 일시 및 장소를 정하여 회의 개최 15일 전까지 분쟁당사자 또는 참고인에게 출석을 통지해야 한다. **제51조의4(조정안에 대한 거부 의사 통지)** 법 제47조제2항에 따라 조정안을 제시받은 당사자는 조정안을 거부하려는 경우에는 조정안을 제시받은 날부터 15일 이내에 인편, 등기우편 또는 전자우편의 방법으로 그 의사를 분쟁조정위원회에 알려야 한다.

3. 개정내용 해설

□ 분쟁조정 의무참여제의 전면 확대(법 제43조제3항)

○ 분쟁조정 신청이 접수되면 특별한 사유*가 없는 한 민간 기업도 분쟁조정에 반드시 응하도록 분쟁조정 의무참여 대상을 공공기관에서 모든 개인정보처리자로 확대하였다.

< 특별한 사유 예시 >

- 분쟁조정 신청인이 분쟁조정을 신청하기 이전에 해당 분쟁조정에 대한 소가 제기된 경우
- 해당 개인정보 관련 분쟁이 분쟁조정 성립, 확정판결, 다른 법률에 따른 분쟁조정기구에 의한 결정 등의 방법으로 이미 종결된 경우
- 당사자가 이미 분쟁조정위원회에서 심의·결정하였거나 조정 전 합의로 종결 처리한 사건을 다시 조정 신청한 경우

○ 분쟁조정위원회는 분쟁조정 신청이 접수되면 그 신청내용을 상대방에게 알려야 하며, 분쟁조정 상대방이 특별한 사유에 해당하여 분쟁조정에 응할 수 없다면 분쟁조정 통지를 받은 날로부터 10일 이내에 불응의사를 분쟁조정위원회에 알려야 한다.

□ 분쟁사건의 사실관계 확인을 위한 사실조사권 신설(법 제45조제2항)

○ 그간의 분쟁조정은 서면 자료와 당사자의 진술에만 의존하여 당사자간의 주장이 대립되는 경우 명확한 사실 확인이 어려워 합리적인 조정안을 마련하기에 어려움이 있었다.

○ 이에 분쟁조정위원회 위원이나 사무기구의 공무원이 분쟁 관련 현장에 출입하여 관련 자료를 열람·조사할 수 있도록 개선하였으며, 사실조사의 공정성 확보를 위해 조사·열람 7일 전까지 문서로 통보하고, 당사자 등이 입회할 수 있도록 하였다.

□ 조정안에 대한 수락 여부를 알리지 않을 경우 수락 간주(법 제47조)

○ 그동안은 분쟁조정 당사자가 분쟁조정위원회의 조정안을 제시받은 날로부터 15일 이내에 수락여부를 회신하지 않으면 거부한 것으로 간주하여 적극적 의사표시에 한계가 있었다.

○ 이에 정보주체의 피해구제를 강화하기 위하여 조정안에 대한 수락 여부 회신이 없을 경우 조정안을 수락한 것으로 간주하도록 개선하고, 조정안을 수락한 것으로 간주될 경우 조정의 내용은 재판상 화해와 동일한 효력을 가지게 되었다.

○ 따라서 분쟁조정 당사자가 조정안을 거부하고자 할 경우에는 조정안을 제시받은 날로부터 15일 이내에 거부 의사를 분쟁조정위원회에 알려야 한다.

□ 그 밖에 개인정보 분쟁조정제도 개선 사항

○ 분쟁조정의 전문성 및 효율성 제고를 위해 위원 정수가 20명에서 30명으로 늘어났으며, 분쟁조정과 관련된 사항을 전문적으로 검토하기 위하여 분쟁조정 전문위원회를 둘 수 있는 규정을 신설하였다.

○ 또한, 분쟁조정위원회는 개인정보 보호 및 정보주체의 권리보호를 위한 개선의견을 보호위원회 및 관계 중앙행정기관에 통보할 수 있도록 하였다.

4. 개인정보처리자 유의사항

□ 분쟁조정에 대한 개정규정*은 2023년 9월 15일 법 시행 이후 분쟁조정 또는 집단분쟁조정이 신청되거나 의뢰되는 경우부터 적용한다.

* 제43조제3항, 제45조제2항부터 4항까지, 제45조의2 및 제47조제3항·제4항

5. 제재 규정

위반행위	제재 내용
제45조제1항에 따른 자료를 정당한 사유 없이 제출하지 아니하거나 거짓으로 제출한 자	1천만원 이하 과태료 (제75조제4항제11호)
제45조제2항에 따른 출입·조사·열람을 정당한 사유 없이 거부·방해 또는 기피한 자	1천만원 이하 과태료 (제75조제4항제12호)

6. 질의 응답

□ 개인정보 분쟁조정이 신청되면 상대방은 반드시 조정에 응하여야 하는지?

⇨ 법 제43조(조정의 신청 등)제3항에 따라 분쟁조정이 신청되었다는 통지를 받은 상대방은 특별한 사유가 없으면 분쟁조정에 응하여야 함
특별한 사유란 분쟁조정 사건 관련 소가 제기된 경우, 동일한 분쟁조정이 개인정보분쟁조정위나 다른 분쟁조정 기구에서 이미 종결된 경우가 해당될 수 있음

□ 개인정보 분쟁조정위원회의 현장 사실조사가 행정처분으로 이어지는 것은 아닌지?

⇨ 법 제60조(비밀유지 등)에 따라 분쟁조정 업무에 조사하거나 하였던 자는 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용하여서는 안 됨
따라서 분쟁조정을 위한 현장 사실조사는 분쟁조정에만 이용됨

□ 조정안에 대하여 당사자는 수락 여부를 15일 이내에 분쟁조정위원회에 반드시 알려야 하는지?

⇨ 법 제47조(분쟁의 조정)제3항, 시행령 제51조의4(조정안에 대한 거부의사 통지)에 따라 분쟁조정위원회의 조정안을 제시받은 당사자는 제시받은 날로부터 15일 이내에 인편, 등기우편, 전자우편의 방법으로 수락 여부를 분쟁조정위에 알려야 함
만일 15일 이내에 수락 여부를 알리지 아니하면 조정안을 수락한 것으로 간주하게 되고, 이는 재판상 화해의 효력을 지니게 되어 더 이상 소송을 통해서도 구제받을 수 없게 됨
따라서 조정안을 수락하지 않는 경우에도 반드시 거부 의사를 조정안을 제시받은 날로부터 15일 이내에 분쟁조정위원회에 알려야 함

8 과징금·형벌·과태료 등 제재 규정 정비

1 과징금 (법 제64조의2)

1. 개정 개요

□ 글로벌 법제와의 정합성 확보를 위해 온·오프라인 개인정보 보호 기준을 일원화하고, 수탁자 처분 조항 도입 등으로 규제 공백 및 불균형을 해소할 수 있도록 하였다.

□ 아울러, 경미한 위반행위에 대하여는 과징금 면제까지 가능하도록 과징금 면제 요건을 신설하고 구체화하여 합리성을 제고하였다.

2. 법령

법률	**제64조의2(과징금의 부과)** ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보처리자에게 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 20억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 1. 제15조제1항, 제17조제1항, 제18조제1항·제2항(제26조제8항에 따라 준용되는 경우를 포함한다) 또는 제19조를 위반하여 개인정보를 처리한 경우 2. 제22조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 처리한 경우 3. 제23조제1항제1호(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 정보주체의 동의를 받지 아니하고 민감정보를 처리한 경우 4. 제24조제1항·제24조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고유식별정보 또는 주민등록번호를 처리한 경우 5. 제26조제4항에 따른 관리·감독 또는 교육을 소홀히 하여 수탁자가 이 법의 규정을 위반한 경우 6. 제28조의5제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우 7. 제28조의8제1항(제26조제8항 및 제28조의11에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 국외로 이전한 경우 8. 제28조의9제1항(제26조제8항 및 제28조의11에 따라 준용되는 경우를 포함한다)을 위반하여 국외 이전 중지 명령을 따르지 아니한 경우 9. 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우. 다만, 개인정보가 분실·도난·유출·위조·변조·훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다. ② 보호위원회는 제1항에 따른 과징금을 부과하려는 경우 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 과징금을 산정한다. ③ 보호위원회는 제1항에 따른 과징금을 부과하려는 경우 개인정보처리자가 정당한 사유 없이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 개인정보처리자의

	전체 매출액을 기준으로 산정하되 해당 개인정보처리자 및 비슷한 규모의 개인정보처리자의 개인정보 보유 규모, 재무제표 등 회계자료, 상품·용역의 가격 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다. ④ 보호위원회는 제1항에 따른 과징금을 부과하는 경우에는 위반행위에 상응하는 비례성과 침해 예방에 대한 효과성이 확보될 수 있도록 다음 각 호의 사항을 고려하여야 한다. 1. 위반행위의 내용 및 정도 2. 위반행위의 기간 및 횟수 3. 위반행위로 인하여 취득한 이익의 규모 4. 암호화 등 안전성 확보 조치 이행 노력 5. 개인정보가 분실·도난·유출·위조·변조·훼손된 경우 위반행위와의 관련성 및 분실·도난·유출·위조·변조·훼손의 규모 6. 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치의 이행 여부 7. 개인정보처리자의 업무 형태 및 규모 8. 개인정보처리자가 처리하는 개인정보의 유형과 정보주체에게 미치는 영향 9. 위반행위로 인한 정보주체의 피해 규모 10. 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력 11. 보호위원회와의 협조 등 위반행위를 시정하기 위한 조치 여부 ⑤ 보호위원회는 다음 각 호의 어느 하나에 해당하는 사유가 있는 경우에는 과징금을 부과하지 아니할 수 있다. 1. 지급불능·지급정지 또는 자본잠식 등의 사유로 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우 2. 본인의 행위가 위법하지 아니한 것으로 잘못 인식할 만한 정당한 사유가 있는 경우 3. 위반행위의 내용·정도가 경미하거나 산정된 과징금이 소액인 경우 4. 그 밖에 정보주체에게 피해가 발생하지 아니하였거나 경미한 경우로서 대통령령으로 정하는 사유가 있는 경우 ⑥ 제1항에 따른 과징금은 제2항부터 제5항까지를 고려하여 산정하되, 구체적인 산정기준과 산정절차는 대통령령으로 정한다. ⑦ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다. ⑧ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니한 경우에는 기간을 정하여 독촉하고, 독촉으로 지정한 기간 내에 과징금과 제7항에 따른 가산금을 내지 아니하면 국세강제징수의 예에 따라 징수한다. ⑨ 보호위원회는 법원의 판결 등의 사유로 제1항에 따라 부과된 과징금을 환급하는 경우에는 과징금을 낸 날부터 환급하는 날까지의 기간에 대하여 금융회사 등의 예금이자율 등을 고려하여 대통령령으로 정하는 이자율을 적용하여 계산한 환급가산금을 지급하여야 한다. ⑩ 보호위원회는 제9항에도 불구하고 법원의 판결에 따라 과징금 부과처분이 취소되어 그 판결 이유에 따라 새로운 과징금을 부과하는 경우에는 당초 납부한 과징금에서 새로 부과하기로 결정한 과징금을 공제한 나머지 금액에 대해서만 환급가산금을 계산하여 지급한다.
시행령	**제60조의2(과징금의 산정기준 등)** ① 법 제64조의2제1항 각 호 외의 부분 본문에 따른 전체 매출액은 위반행위가 있었던 사업연도(이하 이 조에서 "해당사업연도"라 한다) 직전 3개 사업연도의 해당 개인정보처리자의 연평균 매출액으로 한다. 다만, 해당사업연도의 첫날 현재 사업을 개시한 지 3년이 되지 않은 경우에는 그 사업개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액으로 하며, 해당사업연도에 사업을 개시한 경우에는 사업개시일부터 위반행위일까지의 매출액을 연매출액으로 환산한 금액으로 한다. ② 법 제64조의2제1항 각 호 외의 부분 단서에서 "대통령령으로 정하는 경우"란 다음 각 호의

	어느 하나에 해당하는 경우를 말한다. 1. 다음 각 목의 어느 하나에 해당하는 사유로 영업실적이 없는 경우 가. 영업을 개시하지 않은 경우 나. 영업을 중단한 경우 다. 수익사업을 영위하지 않는 등 가목 및 나목에 준하는 경우 2. 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우 ③ 법 제64조의2제2항에 따른 위반행위와 관련이 없는 매출액은 제1항에 따른 전체 매출액 중 다음 각 호의 어느 하나에 해당하는 금액으로 한다. 1. 개인정보의 처리와 관련이 없는 재화 또는 서비스의 매출액 2. 제4항에 따라 제출받은 자료 등에 근거하여 보호위원회가 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 재화 또는 서비스의 매출액이 아닌 것으로 인정하는 매출액 ④ 보호위원회는 제1항부터 제3항까지의 규정에 따른 매출액 산정 등을 위하여 재무제표 등의 자료가 필요한 경우 20일 이내의 기간을 정하여 해당 개인정보처리자에게 관련 자료의 제출을 요청할 수 있다. ⑤ 법 제64조의2제5항제4호에서 "대통령령으로 정하는 사유가 있는 경우"란 해당 개인정보처리자가 위반행위를 시정하고 보호위원회가 정하여 고시하는 기준에 해당되는 경우를 말한다. ⑥ 법 제64조의2제6항에 따른 과징금의 산정기준과 산정절차는 별표 1의5와 같다. **제60조의3(과징금의 부과 및 납부)** ① 보호위원회는 법 제64조의2에 따라 과징금을 부과하려는 경우에는 해당 위반행위를 조사·확인한 후 위반사실·부과금액·이의 제기 방법 및 이의 제기 기간 등을 서면으로 명시하여 과징금 부과대상자에게 통지해야 한다. ② 제1항에 따라 통지를 받은 자는 통지를 받은 날부터 30일 이내에 보호위원회가 지정하는 금융기관에 과징금을 납부해야 한다. ③ 제2항에 따라 과징금의 납부를 받은 금융기관은 과징금을 납부한 자에게 영수증을 발급해야 한다. ④ 금융기관이 제2항에 따라 과징금을 수납한 때에는 지체 없이 그 사실을 보호위원회에 통보해야 한다. **제60조의4(과징금의 납부기한 연기 및 분할 납부)** ① 보호위원회는 법 제64조의2제1항에 따른 과징금의 납부기한을「행정기본법」제29조 및 같은 법 시행령 제7조에 따라 연기하는 경우에는 원래 납부기한의 다음 날부터 2년을 초과할 수 없다. ② 보호위원회는 법 제64조의2제1항에 따른 과징금을「행정기본법」제29조 및 같은 법 시행령 제7조에 따라 분할 납부하게 하는 경우에는 각 분할된 납부기한 간의 간격은 6개월을 초과할 수 없으며, 분할 횟수는 6회를 초과할 수 없다. ③ 제1항 및 제2항에서 규정한 사항 외에 과징금 납부기한 연기 및 분할 납부 신청 등에 필요한 사항은 보호위원회가 정하여 고시한다. **제60조의5(환급가산금의 이자율)** 법 제64조의2제9항에서 "대통령령으로 정하는 이자율"이란「국세기본법 시행령」제43조의3제2항 본문에 따른 이자율을 말한다.
	[별표 1의5] 과징금의 산정기준과 산정절차(제60조의2제6항 관련) 1. 과징금의 산정단계 과징금은 법 제64조의2제4항 각 호에 따른 고려 사항과 이에 영향을 미치는 행위를 종합적으로 고려하여 제2호가목에 따라 산정된 기준금액에 같은 호 나목에 따른 1차 조정, 같은 호 다목에 따른 2차 조정, 같은 호 라목에 따른 부과과징금 결정을 순차적으로 거쳐 산정한다. 다만, 가중하는 경우에도 법 제64조의2제1항 각 호 외의 부분에 따른 과징금 금액의 상한을 넘을 수 없다. 2. 과징금의 산정단계에 따른 산정방식과 고려 사유 가. 기준금액의 산정 1) 기준금액은 제60조의2제1항에 따른 전체 매출액에서 같은 조 제3항에 따른 위반행위와 관련이 없는 매출액을 제외한 매출액에 위반행위의 중대성에 따라 다음과 같이 구분된 과징금의 산정비율(이하 "부과기

준율"이라 한다)을 곱하여 산출한 금액으로 한다.

위반행위의 중대성	부과기준율
매우 중대한 위반행위	2.1% 이상 2.7% 이하
중대한 위반행위	1.5% 이상 2.1% 미만
보통 위반행위	0.9% 이상 1.5% 미만
약한 위반행위	0.03% 이상 0.9% 미만

2) 제60조의2제2항 각 호의 어느 하나에 해당하는 경우에는 1)에도 불구하고 위반행위의 중대성에 따라 기준금액을 다음과 같이 한다.

위반행위의 중대성	기준금액
매우 중대한 위반행위	7억원 이상 18억원 이하
중대한 위반행위	2억원 이상 7억원 미만
보통 위반행위	5천만원 이상 2억원 미만
약한 위반행위	5백만원 이상 5천만원 미만

3) 위반행위의 중대성은 다음의 사항을 종합적으로 고려하여 판단한다.

가) 위반행위의 내용 및 정도

나) 암호화 등 안전성 확보 조치 이행 노력

다) 개인정보가 분실・도난・유출・위조・변조・훼손된 경우 위반행위와의 관련성 및 분실・도난・유출・위조・변조・훼손의 규모

라) 개인정보처리자가 처리하는 개인정보의 유형과 정보주체에게 미치는 영향

마) 위반행위로 인한 정보주체의 피해 규모

나. 1차 조정

위반행위의 기간 및 횟수, 위반행위로 인하여 취득한 이익의 규모, 개인정보처리자의 업무 형태 및 규모를 고려하여 가목에 따른 기준금액의 100분의 90의 범위에서 보호위원회가 정하여 고시하는 기준에 따라 가중하거나 감경할 수 있다.

다. 2차 조정

다음의 사항(법 제64조의2제4항 각 호의 사항 중 가목에 따른 기준금액 산정 및 나목에 따른 1차 조정 단계에서 고려된 사항은 제외한다)을 종합적으로 고려하여 1차 조정을 거친 금액의 100분의 50의 범위에서 보호위원회가 정하여 고시하는 기준에 따라 가중하거나 감경할 수 있다.

1) 보호위원회와의 협조 등 위반행위를 시정하기 위한 조치 여부

2) 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치의 이행 여부

3) 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력

4) 위반행위의 주도 여부

5) 위반행위자가 위반행위 사실의 자진신고 여부

라. 부과과징금의 결정

1) 다음의 사항을 고려하여 다목에 따라 산정된 과징금이 과중하다고 인정되는 경우에는 해당 금액의 100분의 90 범위에서 감경할 수 있다.

가) 위반행위자의 현실적인 부담능력

나) 경제위기 등으로 위반행위자가 속한 시장・산업 여건이 현저하게 변동되거나 지속적으로 악화된 상태인지 여부

2) 법 제64조의2제5항 각 호의 어느 하나에 해당하는 경우에는 과징금을 부과하지 않을 수 있다.

3. 세부 기준

매출액의 산정에 관한 세부 기준, 위반행위의 중대성 판단 기준, 1차 조정 및 2차 조정을 위한 세부 기준, 부과과징금의 결정을 위한 세부 기준과 그 밖에 과징금의 부과에 필요한 사항은 보호위원회가 정하여 고시한다.

3. 개정내용 해설

□ 일반규정과 정보통신서비스 제공자 특례에 산재되어 있는 과징금 규정을 일원화하여 과징금 부과 대상자를 전체 개인정보처리자로 확대하고 수탁자도 과징금 부과대상에 포함하였다.

※ 종전법은 가명정보(§28의6), 주민등록번호 유출(§34의2), 정보통신서비스 제공자 특례(§39의15)에서 분산하여 과징금을 규정, 수탁자의 법 위반에 대한 과징금 부과 근거 규정 없음

○ 과징금 대상 위반행위로 고유식별정보·주민번호 처리 위반, 국외 이전 중지 명령 위반을 추가하였으며, 주요 내용은 다음과 같다.

<table>
<tr><th colspan="2">과징금(각 호 기준)</th><th rowspan="2">비 고</th></tr>
<tr><th>종전(특례 기준)</th><th>개정(9개)</th></tr>
<tr><td>6. 동의없이 수집(§39의3①)</td><td rowspan="2">1. 수집·이용·제공 위반
(§15①, §17①, §18①·②, §19)</td><td rowspan="2">삭제 : 동의 항목 고지 위반(§17②)
추가 : 수집 위반(§15①)</td></tr>
<tr><td>1. 이용·제공 위반
(§17①·②, §18①·②, §19)</td></tr>
<tr><td>2. 동의없이 아동 개인정보 수집(§22⑥)</td><td>2. 동의없이 아동 개인정보 처리(§22의2①)</td><td></td></tr>
<tr><td>3. 동의없이 민감정보 수집(§23①1)</td><td>3. 동의없이 민감정보 처리(§23①1)</td><td></td></tr>
<tr><td>개정법 신설</td><td>4. 고유식별정보, 주민번호 처리 위반
(§24①, §24의2①)</td><td>현행 : 벌칙(고유식별정보), 과태료(주민번호)에서 규정
⇒ 과징금 규정도 신설</td></tr>
<tr><td>4. 수탁자 관리 소홀(§26④)</td><td>5. 수탁자 관리 소홀(§26④)</td><td></td></tr>
<tr><td>(전체 처리자) 가명정보 재식별 금지 위반(§28의5①)</td><td>6. 가명정보 재식별 금지 위반(§28의5①)</td><td></td></tr>
<tr><td>7. 동의없이 국외 이전(§39의12② 본문)</td><td>7. 국외 이전 위반(§28의8①)</td><td>동의 외
국외 이전 허용 요건 다양화</td></tr>
<tr><td>개정법 신설</td><td>8. 국외 이전 중지 명령 위반(§28의9①)</td><td></td></tr>
<tr><td>5. (정보통신서비스 제공자) 개인정보 유출 + 안전조치 미비(§29)</td><td rowspan="2">9. 개인정보 유출 + 안전조치 미비(§29)</td><td rowspan="2">적용 대상을
개인정보처리자가 처리하는 모든 개인정보로 확대</td></tr>
<tr><td>(개인정보처리자) 주민번호 유출 + 안전조치 미비(§24③)</td></tr>
</table>

□ 과징금은 위반행위의 내용 및 정도, 위반행위의 기간 및 횟수 등 법 제64조의2제4항 각 호에 따른 고려사항과 이에 영향을 미치는 행위를 종합적으로 고려하여 다음과 같이 기준금액에 1차 조정, 2차 조정, 부과과징금 결정을 순차적으로 거쳐 산정한다.

기준금액 산정	→	1차 조정	→	2차 조정	→	부과 과징금의 결정	⇒	과징금 부과금액

○ 다만, 가중하는 경우에도 과징금 부과 상한인 전체 매출액의 3% 또는 정액 과징금의 경우 20억원을 넘을 수 없다.

※ 종전 법(정보통신서비스 제공자 특례 기준)상 상한은 위반행위와 관련된 매출액의 3% 또는 4억원

□ 매출액 산정의 기준금액을 정할 때에는 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액에 위반행위의 중대성에 따라 구분된 과징금의 산정비율(부과기준율)을 곱하여 산출한 금액으로 한다.

○ 위반행위와 관련이 없는 매출액은 ① 개인정보의 처리와 관련이 없는 재화 또는 서비스의 매출액, ② 제출받은 자료 등에 근거하여 보호위원회가 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 재화 또는 서비스의 매출액이 아닌 것으로 인정하는 매출액을 의미한다.

○ 개인정보처리자가 정당한 사유 없이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 개인정보처리자의 전체 매출액을 기준으로 산정하되 재무제표 등에 근거하여 매출액을 추정할 수 있다.

□ 영업 미개시, 영업 중단 또는 수익사업을 영위하지 않는 등의 사유로 영업실적이 없거나 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우에는 정액 과징금이 부과된다.

□ 위반행위의 중대성은 위반행위의 내용 및 정도 등을 종합적으로 고려하여 판단하며, 중대성 별로 정한 부과기준율 및 기준금액(정액 과징금)은 다음과 같다.

위반행위의 중대성	부과기준율	기준금액(정액 과징금)
매우 중대한 위반행위	2.1% 이상 2.7% 이하	7억원 이상 18억원 이하
중대한 위반행위	1.5% 이상 2.1% 미만	2억원 이상 7억원 미만
보통 위반행위	0.9% 이상 1.5% 미만	5천만원 이상 2억원 미만
약한 위반행위	0.03% 이상 0.9% 미만	5백만원 이상 5천만원 미만

※ (위반행위 중대성 판단기준) 위반행위의 내용 및 정도, 암호화 등 안전성 확보 조치 이행 노력, 개인정보가 유출 등이 된 경우 위반행위와의 관련성 및 유출 등의 규모, 개인정보처리자가 처리하는 개인정보의 유형과 정보주체에게 미치는 영향, 위반행위로 인한 정보주체의 피해 규모

□ 1차 조정으로 위반행위의 기간 및 횟수, 위반행위로 인하여 취득한 이익의 규모 등을 고려하여 다음과 같이 기준금액을 가중·감경할 수 있다.

구분	가중	감경
비율	(종전) 50% 이내 → (개정) 90% 이내	(종전) 50% 이내 → (개정) 90% 이내
고려 사항	(현행 유지) △위반 기간 (신설) △위반 횟수(감경에서 가중으로 전환)	(신설) △위반으로 취득한 이익, △개인정보 처리자의 업무 형태·규모

□ 2차 조정으로 보호위원회와의 협조 등 위반행위를 시정하기 위한 조치 여부, 개인정보 보호를 위한 노력 등을 고려하여 다음과 같이 1차 조정을 거친 금액을 가중·감경할 수 있다.

구분	가중	감경
비율	50% 이내	50% 이내
고려 사항	(현행 유지) △조사 방해, △위반 주도 여부	(현행 유지) △조사 협조, △인증 등 자율보호, △자진신고 (신설) △자진 시정, △피해 회복 및 피해 확산 방지

□ 위반행위자의 현실적인 부담능력 등을 고려하여 산정된 과징금이 과중하다고 인정되는 경우에는 2차 조정을 거친 금액의 90% 이내에서 감경할 수 있으며,

○ 과징금 부과 대상 중 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우, 본인의 행위가 위법하지 않은 것으로 잘못 인식할 만한 정당한 사유가 있는 경우, 위반행위가 경미하거나 산정된 과징금이 소액인 경우 등에는 과징금을 부과하지 않을 수 있다.

□ 과징금 납부기한 연기 및 분할 납부 근거를 대통령령으로 상향하였으며, 최대 2년 간 납부기한 연기, 최대 6회 분할 납부할 수 있도록 하였다.

□ 보호위원회는 개인정보 보호법 개정에 따른 후속 조치로 「개인정보 보호법 위반에 대한 과징금 부과기준」 고시 제정(2023.9.15. 시행)을 통해 과징금 미부과 및 위반행위의 중대성 판단기준 구체화, 가중·감경 사유 및 비율 조정 등 시행에 필요한 사항을 규정하였다.

4. 개인정보처리자 유의사항

□ 과징금 부과에 있어 시행 전에 종료된 위반행위에 대해서는 종전의 규정(제28조의6, 제34조의2, 제69조의15)을 적용하지만, 2023년 9월 15일 법 시행 당시 종료되지 아니한 위반행위에 대한 과징금 부과는 법 제64조의2의 개정규정을 적용한다.

5. 제재 규정

□ 납부기한까지 과징금을 내지 않으면 납부기한의 다음 날부터 내지 않은 과징금의 연 6%에 해당하는 가산금을 징수한다. 가산금 기간은 60개월을 초과하지 못한다.

6. 질의 응답

□ 법 시행 전 위반행위에 적용되는 과징금 규정은?

⇨ 시행 전에 종료된 위반행위는 종전 규정(제28조의6, 제34조의2 및 제39조의15)을 적용, 종료되지 않은 위반행위는 개정법을 적용

※ 개인정보 보호법 부칙 제8조(과징금 부과에 관한 경과조치 등)

□ 위반행위와 관련이 없는 매출액 판단 시 어떠한 사항을 고려할 수 있는지?

⇨ 다음의 사항을 종합적으로 고려할 수 있음

1. 재화·서비스의 종류·성질, 공급 또는 제공 방식 등에 따른 독자성과 부속성의 정도
2. 재화·서비스를 이용하는 정보주체가 별개의 재화·서비스로 합리적으로 인식 가능한 정도
3. 위반행위의 대상이 된 개인정보의 범주·특성
4. 개인정보파일·개인정보처리시스템의 관리·운영 방식의 분리 또는 연계 여부 등 독자성의 정도
5. 개인정보 처리방침 또는 이용계약·약관 등에서 규정한 재화·서비스의 범위
6. 통계청장이 고시하는 「한국표준산업분류」상 분류 또는 위반행위자의 품목별 또는 업종별 매출액 등의 회계단위
7. 그 밖에 제1호부터 제6호까지에 준하는 사항

□ 정액 과징금 대상인 수익사업을 영위하지 않는 경우의 기준은?

⇨ 공공기관, 비영리법인, 비영리단체 등으로서 매출액을 산정하지 않고, 「법인세법」 제4조 제3항제1호에 따른 수익사업에서 생기는 소득이 없는 경우를 의미

□ 관련 없는 매출액 입증과 관련하여 사업자가 행사할 수 있는 절차는?

⇨ 개인정보 보호법 시행령 및 「위원회 조사 및 처분에 관한 규정」에 따라 사업자는 입증자료 또는 의견제출을 통해 위반행위와 관련 없는 매출액을 주장할 수 있음

참고 **개인정보 보호법 위반에 대한 과징금 부과기준('23.9.15. 시행)**

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제64조의2제6항, 같은 법 시행령(이하 "영"이라 한다) 제60조의2 및 [별표 1의5]에 따른 과징금 부과에 필요한 세부 기준을 정함을 목적으로 한다.

제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음과 같다.

1. "위반행위"란 법을 위반하여 법 제64조의2제1항 각 호에 따른 과징금 부과 대상이 되는 행위를 말한다.
2. "기준금액"이란 과징금 산정의 기초로서 영 제60조의2제1항에 따른 전체 매출액(이하 "전체 매출액"이라 한다)에서 같은 조 제3항에 따른 위반행위와 관련이 없는 매출액(이하 "위반행위와 관련이 없는 매출액"이라 한다)을 제외한 매출액에 영 [별표 1의5] 제2호가목 1)에서 위반행위의 중대성 별로 정한 부과기준율(이하 "부과기준율"이라 한다)을 곱하여 산출한 금액 또는 영 제60조의2제2항 및 [별표 1의5] 제2호가목 2)에서 정한 금액을 말한다.
3. "1차 조정"이란 위반행위의 기간 및 횟수, 위반행위로 인하여 취득한 이익의 규모, 개인정보처리자의 업무 형태 및 규모를 고려하여 기준금액의 100분의 90의 범위에서 가중하거나 감경하는 것을 말한다.
4. "2차 조정"이란 다음 각 목의 사항(법 제64조의2제4항 각 호의 사항 중 기준금액 산정 및 1차 조정 단계에서 고려된 사항은 제외한다)을 종합적으로 고려하여 1차 조정을 거친 금액의 100분의 50의 범위에서 가중하거나 감경하는 것을 말한다.
   가. 개인정보 보호위원회(이하 "보호위원회"라 한다)와의 협조 등 위반행위를 시정하기 위한 조치 여부
   나. 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치의 이행 여부
   다. 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력
   라. 위반행위의 주도 여부
   마. 위반행위자가 위반행위 사실의 자진신고 여부
5. "부과과징금의 결정"이란 기준금액에 1차 조정과 2차 조정을 거친 금액이 위반행위자의 현실적 부담능력 등을 종합적으로 고려하여 과중하다고 인정되는 경우 등에 2차 조정을 거친 금액을 그 금액의 100분의 90의 범위에서 감경하거나 면제하는 것을 말한다.

제3조(위반기간의 산정) ① 위반기간은 위반행위의 개시일부터 종료일까지의 기간을 말한다. 다만, 위반행위가 과징금 부과처분을 명하는 보호위원회의 심의종결일까지 종료되지 아니한 경우에는 해당 사건에 대한 보호위원회의 심의종결일을 위반행위의 종료일로 본다.

② 제1항에 따른 위반기간을 산정하면서 위반행위의 개시일 또는 종료일이 불분명한 경우에는 위반행위자의 영업·재무 관련 자료, 임직원·정보주체 등의 진술, 동종·유사 업종을 영위하는 다른 개인정보처리자의 영업 및 거래실태·관행 등을 고려하여 이를 산정할 수 있다.

제4조(과징금 부과 여부의 결정) ① 본인의 행위가 위법하지 않은 것으로 잘못 인식할 만한 정당한 사유가 있는 경우에는 과징금을 부과하지 않는다.

② 다음 각 호의 어느 하나에 해당하는 경우에는 과징금을 부과하지 않을 수 있다. 다만, 본문에 따라 과징금 부과처분을 받지 않은 자가 그 결정이 있은 날부터 3년 이내에 같은 위반행위를 하는 경우에는 그렇지 않다.

1. 위반행위의 내용·정도가 경미하거나 사소한 부주의나 오류로 인한 위반행위인 경우
2. 정보주체에게 피해가 발생하지 아니하였거나 경미한 경우로서 위반행위자가 위반행위를 시정하고 법 제34조에 따른 개인정보 유출 등의 통지·신고를 위반하지 않은 경우

제5조(과징금의 부과기준) ① 과징금 부과금액은 법 제64조의2제4항 각 호에 따른 고려 사항과 이에 영향을 미치는 행위를 종합적으로 고려하여 기준금액에 1차 조정, 2차 조정, 부과과징금의 결정을 순차적으로 거쳐 산정한다.

② 하나의 행위가 2 이상의 위반행위에 해당하는 경우에는 각 위반행위 별로 산정된 과징금 중 가장 큰 금액을 기준으로 과징금을 부과한다.

제6조(기준금액) ① 기준금액은 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액에 부과기준율을 곱한 금액으로 정한다.

② 영 제60조의2제2항 각 호의 어느 하나에 해당하여 제1항을 적용할 수 없는 경우에는 영 [별표 1의5] 제2호가목 2)에 따라 기준금액을 정한다.

③ 다음 각 호의 경우에는 영 제60조의2제2항 각 호의 어느 하나에 해당하여 매출액이 없거나 매출액의 산정이 곤란한 경우로 본다.

1. 공공기관, 비영리법인, 비영리단체 등으로서 매출액을 산정하지 않고,「법인세법」 제4조제3항제1호에 따른 수익사업에서 생기는 소득이 없는 경우
2. 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 결과 산정된 매출액이 없는 경우

제7조(매출액 산정기준 판단 시 고려사항) ① 전체 매출액은 총매출액에서 부가가치세, 매출할인, 매출환입, 매출에누리 등을 차감한 순매출액(업종의 특성에 따라 매출액에 준하는 영업수익 등을 사용하는 경우에는 영업수익 등을 말한다)으로 한다.

② 영 제60조의2제1항 단서에서 정한 직전 3개 사업연도 또는 해당사업연도는 위반행위의 종료일을 기준으로 판정한다.

③ 영 제60조의2제3항에 따라 보호위원회가 위반행위와 관련이 없는 매출액으로 인정하는 매출액의 판단 시에는 다음 각 호의 사항을 종합적으로 고려할 수 있다.

1. 재화·서비스의 종류·성질, 공급 또는 제공 방식 등에 따른 독자성과 부속성의 정도
2. 재화·서비스를 이용하는 정보주체가 별개의 재화·서비스로 합리적으로 인식 가능한 정도
3. 위반행위의 대상이 된 개인정보의 범주·특성
4. 개인정보파일·개인정보처리시스템의 관리·운영 방식의 분리 또는 연계 여부 등 독자성의 정도
5. 개인정보 처리방침 또는 이용계약·약관 등에서 규정한 재화·서비스의 범위
6. 통계청장이 고시하는 「한국표준산업분류」상 분류 또는 위반행위자의 품목별 또는 업종별 매출액 등의 회계단위
7. 그 밖에 제1호부터 제6호까지에 준하는 사항

④ 재화·서비스의 유형·이용 방식 등이 유사하면 공급 또는 제공되는 지역·범위 등에 관계없이 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 재화·서비스로 볼 수 있다.

⑤ 재화·서비스에 대한 매출액은 회계자료를 참고하여 정하되, 위반행위자가 매출액 산정자료를 가지고 있지 않거나 정당한 사유로 제출하지 못하는 경우에는 위반행위자 및 동종 유사 업종을 영위하는 다른 개인정보처리자의 과거 실적, 사업계획, 그 밖에 시장상황 등을 종합적으로 고려하여 매출액을 산정할 수 있다.

제8조(중대성의 판단) ① 영 [별표 1의5] 제2호가목 1) 및 2)에 따른 위반행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준을 기준으로 정한다.

② 제1항에도 불구하고 [별표]에서 고려되지 않거나 [별표]와 다르게 고려할 사유(해당 사유가 가중 또는 감면사유와 중복되는 경우는 제외한다)가 있는 경우에는 위반행위의 중대성의 정도를 달리 정할 수 있다. 이 경우 그 사유를 의결서에 명시하여야 한다.

제9조(1차 조정) ① 위반행위자가 다음 각 호의 어느 하나에 해당하는 경우에는 기준금액에 다음 각 호와 같이 과징금을 가산한다.

1. 위반기간이 1년을 초과하는 경우

가. 위반기간이 1년 초과 2년 이내인 경우 : 기준금액의 100분의 25에 해당하는 금액을 가산

나. 위반기간이 2년을 초과하는 경우 : 기준금액의 100분의 50에 해당하는 금액을 가산

2. 최근 3년간 법 제64조의2제1항 같은 호에 해당하는 행위로 1회 이상 과징금 부과처분을 받은 경우. 이 경우 위반횟수 기간의 계산은 과징금 부과처분을 받은 날과 그 처분 후 다시 해당 위반행위를 하여 적발된 날을 기준으로 한다.

가. 1회 과징금 부과처분을 받은 경우 : 기준금액의 100분의 15에 해당하는 금액을 가산

나. 2회 이상 과징금 부과처분을 받은 경우 : 기준금액의 100분의 30에 해당하는 금액을 가산

② 위반행위자가 다음 각 호의 어느 하나에 해당하는 경우에는 기준금액에 다음 각 호와 같이 과징금을 감경한다.

1. 위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우 : 기준금액의 100분의 30 이하에 해당하는 금액을 감경

2. 위반행위자가 공공기관, 비영리법인, 비영리단체 또는 「중소기업기본법」 제2조에 따른 중소기업자인 경우 등 위반행위자의 업무 형태 및 규모에 비해 과중하다고 인정되는 경우 : 기준금액의 100분의 50 이하에 해당하는 금액을 감경

③ 제1항에서 정한 가중사유 또는 제2항에서 정한 감경사유가 2개 이상 해당되는 경우에는 가중금액을 합산하여 가중하거나 감경금액을 합산하여 감경하되 각 가중·감경의 범위는 기준금액의 100분의 90을 초과할 수 없다.

제10조(2차 조정) ① 위반행위자가 다음 각 호의 어느 하나에 해당하는 경우에는 1차 조정을 거친 금액에 다음 각 호와 같이 추가적으로 과징금을 가산할 수 있다.

1. 위반행위자 및 그 소속 임직원이 법 제63조제1항 및 제2항에 따른 물품·서류의 제출요구 또는 검사를 거부하거나 증거인멸, 은폐, 조작, 허위의 정보제공 등의 방법으로 조사를 방해하거나 관련 정보주체 등에게 허위로 진술하도록 요청한 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 가산

2. 다수의 위반행위자가 관련된 상황에서 위반행위를 주도하거나 선도한 경우 : 1차 조정을 거친 금액의 100분의 20 이하에 해당하는 금액을 가산

② 위반행위자가 다음 각 호의 어느 하나에 해당하는 경우에는 1차 조정을 거친 금액에 다음 각 호와 같이 추가적으로 과징금을 감경할 수 있다.

1. 보호위원회와의 협조 등 위반행위를 시정하기 위하여 조치한 경우로서 다음 각 목의 어느 하나에 해당하는 경우

가. 과징금의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경

나. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경

2. 개인정보 분쟁조정, 민사조정 등을 통해 정보주체에게 발생한 피해에 대한 원상회복, 손해배상 또는 이에 상당하는 필요한 피해의 회복 및 피해 확산 방지 조치를 이행한 경우(다만, 법 제39조의7에 따른 손해배상책임의 이행을 위한 보험 등의 가입은 제외한다) : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경

3. 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위하여 노력한 경우로서 다음 각 목의 어느 하나에 해당하는 경우

가. 개인정보 보호를 위해 보호위원회가 인정하는 인증을 받은 경우 : 1차 조정을 거친 금액의 100분의 50 이하에 해당하는 금액을 감경

나. 개인정보 보호 자율규제 규약을 이행하는 등 개인정보 보호 활동을 성실히 수행한 것으로 확인된 경우 : 1차 조정을 거친 금액의 100분의 40 이하에 해당하는 금액을 감경

다. 개인정보 처리방침의 평가 또는 개인정보 보호수준 평가의 결과가 상위 등급인 경우, 개인정보 영향평가(다만, 법 제33조제1항에 따라 개인정보 영향평가를 해야 하는 경우는 제외한다)를 하는 등 개인정보 보호 활동을 성실히 수행한 것으로 확인된 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경

4. 위반행위 사실을 자진신고(법 제34조제3항 전단에 따른 신고는 제외한다)한 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경

5. 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과징금을 줄일 필요가 있다고 인정되는 경우 : 1차 조정을 거친 금액의 100분의 10 이하에 해당하는 금액을 감경

③ 제1항에서 정한 가중사유 또는 제2항에서 정한 감경사유가 2개 이상 해당되는 경우에는 가중금액을 합산하여 가중하거나 감경금액을 합산하여 감경하되 각 가중·감경의 범위는 1차 조정을 거친 금액의 100분의 50을 초과할 수 없다.

제11조(부과과징금의 결정) ① 위반행위자의 현실적인 부담능력, 위반행위자가 속한 시장·산업 여건 등을 고려하여 제10조에 따라 산정된 과징금이 과중하다고 인정되는 경우에는 다음 각 호와 같이 해당 금액의 100분의 90 범위에서 감경할 수 있다.

1. 위반행위자의 자산, 자기자본 등 재무상황에 비추어 위반행위자가 과징금을 부담할 능력이 현저히 부족하다고 객관적으로 인정되는 경우

2. 경제위기 등으로 위반행위자가 속한 시장·산업 여건이 현저하게 변동되거나 지속적으로 악화된 상태인 경우

② 다음 각 호의 어느 하나에 해당하는 경우에는 제10조에 따라 산정된 과징금을 면제할 수 있다.

1. 위반행위자의 지급불능·지급정지 또는 자본잠식 등의 사유로 위반행위자가 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우

2. 제10조에 따라 산정된 과징금이 다음 각 목의 어느 하나에 해당하는 경우

가. 2백만원 이하인 경우

나. 산정된 과태료 금액보다 적은 경우(위반행위가 법 제75조에 따른 과태료 부과 대상이 되는 행위인 경우에 한한다)

③ 제1항에 따른 위반행위자의 현실적인 부담능력과 관련한 감경은 다음 각 호의 경우에는 적용하지 아니한다.

1. 보호위원회로부터 부과받을 과징금 납부로 인해 단순히 자금 사정에 어려움이 예상되는 경우

2. 위반행위자가 현실적인 부담능력 입증과 관련된 객관적인 자료를 제출하지 않은 경우

④ 부과과징금이 법정 한도액을 넘는 경우에는 법정 한도액을 부과과징금으로 한다.

⑤ 부과과징금이 1억원 이상인 경우에는 1백만원 단위 미만의 금액을, 1억원 미만인 경우에는 1십만원 단위 미만의 금액을 버리는 것을 원칙으로 한다. 다만, 보호위원회는 부과과징금의 규모를 고려하여 적당하다고 생각되는 금액 단위 미만의 금액을 버리고 부과과징금을 결정할 수 있다.

⑥ 과징금 부과의 기준이 되는 매출액 등이 외국환을 기준으로 산정되는 경우에는 해당 매출액 등 산정 기간의 평균환율을 적용하여 원화로 환산한 금액을 부과과징금으로 한다. 이 경우 환율은 하나은행이 최초로 고시하는 매매기준율에 따르며, 하나은행이 고시하지 않는 외국환의 경우에는 미국 달러화로 환산한 후 이를 원화로 다시 환산한다.

제12조(재검토 기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 9월 15일을 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-3호, 2023. 9. 15.>

제1조(시행일) 이 고시는 2023년 9월 15일부터 시행한다. 다만, 제10조제2항제2호 괄호 부분에 해당하는 개정규정 및 제10조제2항제3호다목의 개정규정은 2024년 3월 15일부터 시행한다.

제2조(시행일에 관한 경과조치) ① 부칙 제1조 단서에 따라 제10조제2항제2호 괄호 부분에 해당하는 개정규정이 시행되기 전까지는 해당 규정은 다음과 같이 규정된 것으로 본다. 다만, 법 제39조의9에 따른 손해배상책임의 이행을 위한 보험 등의 가입은 제외한다.

② 부칙 제1조 단서에 따라 제10조제2항제3호다목의 개정규정이 시행되기 전까지는 해당 규정 중 "개인정보 처리방침의 평가 또는 개인정보 보호수준 평가의 결과가"는 "개인정보 처리방침의 평가의 결과가"로 규정된 것으로 본다.

제3조(과징금의 산정기준에 관한 경과조치) 이 고시 시행 전의 위반행위로 종전 「개인정보보호 법규 위반에 대한 과징금 부과기준」 또는 「주민등록번호 유출 등에 대한 과징금 부과기준」에 따라 받은 행정처분은 제9조제1항제2호의 개정규정에 따른 위반행위의 횟수 산정에 포함한다.

[별표] 위반행위의 중대성 판단기준(제8조제1항 관련)

부과수준 / 고려사항	상	중	하
고의·과실	위반행위가 위반행위자의 고의에 의한 경우 또는 중대한 과실에 의한 경우로서 특히 참작할 사유가 없는 경우	위반행위가 위반행위자의 중대한 과실에 의한 경우로서 특히 참작할 사유가 있는 경우	상 또는 중에 해당되지 않는 경우
위반행위의 방법	위반행위의 방법 및 수단을 고려할 때 부당성이 현저히 큰 경우	위반행위의 방법 및 수단을 고려할 때 부당성이 상당한 경우	상 또는 중에 해당되지 않는 경우
위반행위자가 처리하는 개인정보의 유형	위반행위의 대상이 된 개인정보가 민감정보 또는 고유식별정보인 경우	위반행위의 대상이 된 개인정보가 인증정보인 경우	상 또는 중에 해당되지 않는 경우
위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향	정보주체에게 현저한 피해를 입혔거나 입힐 가능성이 높은 경우	정보주체에게 상당한 피해를 입혔거나 입힐 가능성이 높은 경우	상 또는 중에 해당되지 않는 경우

비고

1. 위반행위의 중대성의 정도는 고려사항별 부과기준을 종합적으로 고려하여 판단한다.
2. 위반행위가 고려사항별 부과수준 중 두 가지 이상에 해당하는 경우에는 높은 부과수준을 적용한다.
3. 고려사항별 부과수준의 판단기준은 다음과 같다.

가. 고의·과실

위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려하여 판단한다.

나. 위반행위의 방법

안전성 확보 조치 이행 노력 여부, 개인정보 보호책임자 등 개인정보 보호 조직, 위반행위가 내부에서 조직적으로 이루어졌는지 여부, 사업주, 대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하여 판단한다. 개인정보가 분실·도난·유출·위조·변조·훼손(이하 "유출등"이라 한다)된 경우에는 개인정보의 유출등과 안전성 확보 조치 위반행위와의 관련성을 포함하여 판단한다.

다. 위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향

피해 개인정보의 규모, 위반기간, 정보주체의 권리·이익이나 사생활 등에 미치는 영향 등을 종합적으로 고려하여 판단한다. 개인정보가 유출등이 된 경우에는 유출등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.

2 공표 및 공표명령(법 제66조)

1. 개정 개요

□ 공표 대상에 과징금 부과를 추가하고, 처분 사실에 대한 정보공개 강화를 위해 처분 등을 받은 자에게 처분 등을 받았다는 사실을 공표할 것을 명령할 수 있는 공표명령 제도가 도입되었다.

2. 법령

법률	**제66조(결과의 공표)** ① 보호위원회는 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제64조의2에 따른 과징금의 부과, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과의 내용 및 결과에 대하여 공표할 수 있다. ② 보호위원회는 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제64조의2에 따른 과징금의 부과, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과처분 등을 한 경우에는 처분 등을 받은 자에게 해당 처분 등을 받았다는 사실을 공표할 것을 명할 수 있다. ③ 제1항 및 제2항에 따른 개선권고 사실 등의 공표 및 공표명령의 방법, 기준 및 절차 등은 대통령령으로 정한다.
시행령	**제61조(결과의 공표)** ① 보호위원회는 법 제66조제1항에 따라 다음 각 호의 사항을 보호위원회 인터넷 홈페이지 등에 게재하여 공표할 수 있다. 1. 위반행위의 내용 2. 위반행위를 한 자 3. 개선권고, 시정조치 명령, 과징금의 부과, 고발, 징계권고, 과태료 부과의 내용 및 결과 ② 보호위원회는 법 제66조제2항에 따라 개선권고, 시정조치 명령, 과징금의 부과, 고발, 징계권고 및 과태료 부과처분 등(이하 이 조에서 "처분등"이라 한다)을 받은 자에게 다음 각 호의 사항을 공표할 것을 명할 수 있다. 이 경우 공표의 내용·횟수, 매체와 지면의 크기 등을 정하여 명해야 하며, 처분등을 받은 자와 공표 문안 등에 관하여 협의할 수 있다. 1. 위반행위의 내용 2. 위반행위를 한 자 3. 처분등을 받았다는 사실 ③ 보호위원회는 제1항에 따라 공표하려는 경우 또는 제2항에 따라 공표할 것을 명하려는 경우에는 위반행위의 내용 및 정도, 위반 기간 및 횟수, 위반행위로 인하여 발생한 피해의 범위 및 결과 등을 고려해야 한다. ④ 보호위원회는 공표 또는 공표명령에 대한 심의·의결 전에 처분등을 받은 자에게 소명자료를 제출하거나 의견을 진술할 수 있는 기회를 주어야 한다.

3. 개정내용 해설

□ 공표 대상 처분에 법 제64조의2에 따른 과징금의 부과를 공표 대상 처분으로 추가하였으며,

○ 개인정보 보호법 위반 등 행정조치를 받은 개인정보처리자에 대해 자신의 홈페이지 등에 해당사실을 공표하도록 함으로써 개인정보 보호에 대한 경각심을 제고하고 대국민 정보제공을 통해 재발방지와 제재처분의 실효성을 확보하게 되었다.

○ 시행령에 공표명령 기준·절차 등(고려사항, 방법, 문안 등 협의)을 규정하고, 공표명령 대상자에게 소명자료를 제출하거나 의견을 진술할 수 있는 기회를 부여하도록 하였다.

□ 아울러, 개인정보보호위원회가 중앙행정기관으로 출범함에 따라 관계 중앙행정기관의 장이 소관 법률에 규정이 있어야만 공표할 수 있도록 한 규정을 삭제하였다.

□ 보호위원회는 개인정보 보호법 개정에 따른 후속 조치로 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」 제정(2023.10.11. 시행)을 통해 공표명령 규정 신설에 따른 요건 구체화, 공표 요건 및 기간의 조정 등 시행에 필요한 사항을 규정하였다.

참고 **개인정보 보호법 위반에 대한 공표 및 공표명령 지침'23.10.11. 시행**

제1장 총칙

제1조(목적) 이 지침은 개인정보 보호위원회(이하 "보호위원회"라 한다)가 「개인정보 보호법」(이하 "법"이라 한다) 제66조 및 같은 법 시행령(이하 "영"이라 한다) 제61조에 따라 개선권고, 시정조치 명령, 과징금의 부과, 고발, 징계권고 및 과태료 부과의 내용 및 결과(이하 "처분결과"라 한다)를 공표하려는 경우 또는 처분 등을 받은 자에게 처분 등을 받았다는 사실을 공표할 것을 명하려는 경우에 있어 필요한 사항을 정함으로써 공표제도를 효율적으로 운영하고 공표효과를 높이는 데 그 목적이 있다.

제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "중앙일간지"란 「신문 등의 진흥에 관한 법률」 제2조제1호에서 정한 일간신문 중 서울에 발행소를 두고 전국을 대상으로 발행되는 신문을 말한다.
2. "지방일간지"란 「신문 등의 진흥에 관한 법률」 제2조제1호에서 정한 일간신문 중 서울을 제외한 특정지역에 발행소를 두고 특정지역을 대상으로 발행되는 신문을 말한다.
3. "잡지"란 「잡지 등 정기간행물의 진흥에 관한 법률」 제2조제1호에서 정한 동일한 제호로 월 1회 이하 정기적으로 발행되는 책자 형태의 간행물을 말한다.

제2장 법 위반행위에 대한 공표

제3조(공표요건) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우 처분결과를 공표할 수 있다.

1. 보호위원회가 정한 고발 기준에 해당하여 위반행위를 한 자를 고발하는 경우
2. 보호위원회의 처분 시점을 기준으로 최근 3년 내 시정조치 명령, 과태료, 과징금 부과처분을 2회 이상 받은 경우

② 제1항에도 불구하고 보호위원회는 위반행위의 고의성, 개인정보 침해의 정도 및 피해규모, 사업규모 등 법 준수의 기대가능성, 과거 법 위반 이력, 추가피해의 방지, 피해자에 대한 보상 등 위반행위의 결과제거를 위한 노력, 향후 동종 위반행위의 발생을 방지하기 위한 노력, 위반행위자의 조사협력 및 자진시정 여부 등을 종합적으로 고려하여 공표하지 않을 수 있다.

제4조(공표내용 및 방법) ① 공표문안은 다음과 같이 정하되, 다수의 처분결과를 동시에 공표할 경우에는 표 등을 활용할 수 있다.

개인정보 보호법 위반 행정처분 결과 공표

개인정보 보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

- o 위반행위를 한 자 : ○○주식회사(소재지 : ○○시 ○○구 ○○동)
- o 위반행위의 내용 : ① 법 제29조에 따른 개인정보 암호화 조치 미흡, ② 법 제○○조에 따른 ○○○ 미이행, ③ 법 제○○조에 따른 ○○○ 위반
- o 행정처분의 내용 및 결과 : ①/② ○○○○년 ○월 ○일 과태료 1,200만원 부과, ③ ○○○○년 ○월 ○일 시정조치 명령

○○○○년 ○월 ○일

개 인 정 보 보 호 위 원 회

개인정보 보호법 위반 행정처분 결과 공표 개인정보 보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
		위반조항	위반내용	처분일자	처분내용
1	○○주식회사	법 제○○조	○○○ 미조치	2023.00.00	시정조치 명령
		법 제○○조 ○○항	○○○ 미이행	2023.00.00	과태료 부과 1,200만원
○○○○년 ○월 ○일 개 인 정 보 보 호 위 원 회					

② 보호위원회는 제1항에 따른 공표문안을 파일 형태로 보호위원회의 인터넷 홈페이지(www.pipc.go.kr) 등에 게재하여 공표할 수 있다.

제5조(공표 기간) 보호위원회가 인터넷 홈페이지등에 공표하는 경우 기간은 1년으로 한다.

제3장 처분 등을 받은 사실의 공표명령

제6조(공표명령 요건) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우 위반행위를 한 자에게 처분등을 받은 사실을 공표하도록 명할 수 있다.

1. 법 제63조 제1항 및 제2항에 따른 자료제출 요구 및 검사를 거부하거나 증거인멸, 은폐, 조작, 허위정보제공 등의 방법으로 조사를 방해하거나, 관련 정보주체 등에게 허위로 진술하도록 요청한 경우
2. 1천 명 이상 정보주체의 고유식별정보 또는 민감정보를 분실·도난·유출·위조·변조·훼손한 행위로 인하여 개선권고, 시정조치 명령, 과징금의 부과, 고발, 징계권고 또는 과태료 부과 처분을 받은 경우
3. 위반행위가 법 제64조의2제1항 각 호의 어느 하나에 해당하여 과징금을 부과받은 경우로서 영 [별표 1의5] 제2호가목에 따른 위반행위의 중대성의 정도가 '매우 중대한 위반행위'에 해당하는 경우
4. 법 제75조제1항 각 호에 해당하는 위반행위를 한 경우
5. 법 제75조제2항 각 호에 해당하는 위반행위를 3개 이상 한 경우
6. 다수의 사업자가 관련된 상황에서 위반행위를 주도하거나 선도한 경우
7. 위반행위 시점을 기준으로 위반상태가 3년을 초과하여 지속된 경우
8. 위반행위로 인하여 피해를 입은 정보주체의 수가 10만 명 이상인 경우
9. 위반행위로 인하여 재산상 손실 등 2차 피해가 발생한 경우
10. 위반행위의 대상이 된 개인정보를 불법적으로 매매한 경우

② 제1항에도 불구하고 보호위원회는 위반행위의 고의성, 개인정보 침해의 정도 및 피해규모, 사업규모 등 법 준수의 기대가능성, 과거 법 위반 이력, 추가피해의 방지, 피해자에 대한 보상 등 위반행위의 결과제거를 위한 노력, 향후 동종 위반행위의 발생을 방지하기 위한 노력, 위반행위자의 조사협력 및 자진시정 여부 등을 종합적으로 고려하여 공표명령을 하지 않을 수 있다.

제7조(공표문안 및 활자 크기) ① 원칙적으로 [별표] 표준 공표 문안 및 활자 크기를 따르도록 한다.

② 공표 제목에는 위반행위를 한 자(정보주체에게 널리 알려진 상호 또는 사업장·영업소·사무소·점포 등(이하 "사업장등"이라 한다) 명칭이 있는 경우에는 병기) 및 법 위반행위의 유형이 명백히 표현되어야 한다.

③ 공표내용에는 당해 법 위반행위와 처분등의 내용을 구체적으로 기재해야 한다.

④ 법 위반행위, 위반행위를 한 자의 성명(법인인 경우에는 법인의 명칭 및 대표자의 성명), 위원회의

표시는 선명하게 부각되도록 활자를 고딕체로 하며 색도를 진하게 해야 한다.

제8조(공표명령 방법) ① 보호위원회는 위반행위를 한 자에 대하여 처분등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분등을 받은 사실 등을 신문·잡지 등 간행물, 사업장등 또는 홈페이지 등에 공표하도록 명할 수 있으며, 처분등을 받은 사실의 조속한 공표 필요성 등을 고려하여 위 기간을 조정할 수 있다.

② 제1항에 따른 공표는 위반행위를 한 자 별로 시행하되, 위반행위를 한 자들이 공동으로 법 위반행위를 한 경우 등 필요한 경우에는 연명으로 공표하도록 명할 수 있다.

③ 위반행위를 한 자는 공표 문안 등에 관하여 보호위원회와 미리 문서로 협의해야 한다.

제9조(신문, 잡지 등 공표) ① 보호위원회는 처분등을 받은 사실의 공표를 명할 신문, 잡지 등을 선정함에 있어 다음 각 호의 사항을 고려할 수 있다.

1. 법 위반행위로 인한 파급 효과를 감안하여 법 위반행위로 처분등을 받은 사실 등을 중앙일간지(전판)(법 위반행위로 인한 파급효과가 전국적인 사건의 경우)나 지방일간지(전판)에 게재토록 할 수 있다. 이 경우 해당사건 의결일을 기준으로 1년간 소급하여 위반행위를 한 자의 신문광고 횟수 또는 광고비 지출이 가장 많은 일간신문(전판)에 게재하는 것을 원칙으로 한다. 다만, 법 위반행위가 특정 신문을 통하여 이루어진 경우에는 당해 신문(전판)에 게재하도록 한다.
2. 위반행위를 한 자가 공표할 신문이 2개 이상인 경우 1개는 제1호의 기준에 의하고, 나머지는 위반행위를 한 자가 선택(전판)할 수 있다. 신문광고 실적이 없는 경우에도 위반행위를 한 자가 게재 신문을 선택하도록 할 수 있다.
3. 법 위반행위로 인한 파급효과가 특정지역에 국한되는 사건은 위반행위를 한 자의 소재지를 발행대상지역으로 하는 지방일간지(전판)에 게재토록 하되 제1호 및 제2호를 준용할 수 있다.
4. 위반행위를 한 자의 법 위반행위의 특성상 특정계층을 상대로 한 신문, 전문지, 영자지, 주간지에 게재하는 것이 더 효과적이라고 판단되는 경우에는 당해지 등에 게재토록 할 수 있다.

② 처분등을 받은 사실 등을 토요일, 일요일, 공휴일을 제외한 평일에 게재토록 한다.

③ 신문의 게재면을 2면, 3면, 사회면, 경제면 중에서 택일하도록 하되, 제7조 각 호의 사항 중 3개 이상 해당할 경우 사회면 또는 경제면 중에서 택일하도록 하고, 스포츠신문인 경우에는 2면, 3면, 또는 사회면 중에서 택일하도록 하되, 제7조 각 호의 사항 중 3개 이상 해당할 경우 2면 또는 3면 중에서 택일하도록 한다.

④ 신문, 잡지 등에 공표를 명함에 있어서 공표 크기, 매체수, 게재횟수에 대하여 원칙적으로 다음과 같이 정한다. 다만, 정보주체의 개인정보를 현저히 침해했다고 판단되는 경우에는 공표 크기를 5단 × 37cm까지 할 수 있다.

제6조제1항 각 호 해당 개수	공표크기	매체수(개)	게재횟수(회)
5개 이상	5단 × 18.5cm 이상	2	1
4개	4단 × 18.5cm 또는 5단 × 15cm 이상	2	1
3개	4단 × 15cm 또는 5단 × 12cm 이상	1	1
1~2개	4단 × 10cm 또는 5단 × 9cm 이상	1	1

제10조(사업장등 공표) ① 위반행위를 한 자의 당해 법 위반행위가 정보주체에게 직접 영향을 주는 경우에는 위반행위를 한 자의 사업장등에 공표하게 할 수 있다.

② 공표장소는 위반행위를 한 자의 사업장등의 정문 출입구, 승강기 입구, 게시판 등 정보주체가 출입

하는 곳 중에서 공표사실을 가장 쉽게 볼 수 있는 곳으로 한다.

③ 공표기간은 원칙적으로 7일 이상 30일 이하의 범위(휴업일 제외)에서 다음과 같이 정하며, 공표크기는 A2사이즈(42cm×59.4cm)로 한다.

제6조제1항 각 호 해당 개수	공표기간(휴업일 제외)
5개 이상	20일 이상 30일 이하
4개	15일 이상 20일 미만
3개	10일 이상 15일 미만
1~2개	7일 이상 10일 미만

④ 보호위원회는 당해 공표장소에 공표문을 부착 또는 게시 등의 형태로 공표하게 하되, 보호위원회의 관인이 날인된 스티커를 공표문에 부착해야 한다.

⑤ 보호위원회는 위반행위를 한 자에게 공표문을 무단훼손하거나 공표장소를 무단변경할 경우 시정명령 불이행으로 처벌될 수 있음을 의결내용과 함께 통지한다.

제11조(인터넷 등 공표) ① 보호위원회는 위반행위를 한 자의 법 위반행위가 인터넷을 통하여 이루어지거나 또는 인터넷으로 공표하는 것이 더 효율적이라고 인정하는 경우 해당 인터넷 매체 또는 위반행위를 한 자의 홈페이지(모바일 어플리케이션을 포함한다)의 초기화면 팝업창에 공표하게 할 수 있다. 다만, '1일간 다시 보지 않기' 기능의 사용 등 팝업창 설정방식 등에 대해서는 해당 웹사이트의 특성을 고려하여 보호위원회와 위반행위를 한 자가 협의하여 정하도록 한다.

② 인터넷 등에 공표함에 있어서 공표기간은 원칙적으로 2일 이상 12일 이하의 범위(휴업일 포함)에서 다음과 같이 정하며, 공표크기는 원칙적으로 해당 홈페이지 전체화면의 6분의1로 하되, 정보주체의 개인정보를 현저히 침해했다고 판단되는 경우에는 그 크기를 홈페이지 전체화면의 2분의1까지 확대 조정할 수 있다.

제6조제1항 각 호 해당 개수	공표기간(휴업일 포함)
5개 이상	10일 이상 12일 이하
4개	7일 이상 10일 미만
3개	5일 이상 7일 미만
1~2개	2일 이상 5일 미만

③ 제8조에도 불구하고, 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 보호위원회와 위반행위를 한 자가 협의하여 정하도록 한다.

부칙 <제정, 2023. 10. 11.>

제1조(시행일) 이 지침은 발령한 날부터 시행한다.

제2조(공표 기준에 관한 경과조치 등) 이 지침은 이 지침 시행 전에 종료된 위반행위에 대해서도 적용한다. 다만, 2023년 9월 15일 전에 종료된 위반행위에 대한 공표 기준은 제3조의 개정규정에도 불구하고 종전 「개인정보 보호위원회 처분결과 공표기준」의 제2조에 따른다.

제3조(공표명령에 관한 경과조치) 이 지침은 2023년 9월 15일 이후 발생한 위반행위에 대해서도 적용한다.

※ 별표는 국가법령정보센터(www.law.go.kr) 참조

③ 형벌(법 제70조, 제71조, 제72조, 제73조)

1. 개정 개요

□ 형벌 중심의 제재를 경제 제재 중심으로 전환하면서 그간 경미한 의무 위반사항까지도 형벌을 규정함으로써 초래된 개인정보 업무담당자의 과중한 부담 및 업무회피 문제를 해소하고자 하였다.

□ 아울러, 수탁자 처벌 조항 도입, 개인정보의 사적 목적 이용 등 중대한 범죄행위에 대한 형벌 도입으로 규제 공백 및 불균형을 개선하였다.

2. 법령

법률	**제70조(벌칙)** 현행과 동일 **제71조(벌칙)** 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알면서도 개인정보를 제공받은 자 2. 제18조제1항·제2항, 제27조제3항 또는 제28조의2(제26조제8항에 따라 준용되는 경우를 포함한다), 제19조 또는 제26조제5항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 3. 제22조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 처리한 자 4. 제23조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 민감정보를 처리한 자 5. 제24조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고유식별정보를 처리한 자 6. 제28조의3제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 관계 중앙행정기관의 장으로부터 전문기관으로 지정받지 아니하고 가명정보를 결합한 자 7. 제28조의3제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 전문기관의 장의 승인을 받지 아니하고 결합을 수행한 기관 외부로 결합된 정보를 반출하거나 이를 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 결합된 정보를 제공받은 자 8. 제28조의5제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 특정 개인을 알아보기 위한 목적으로 가명정보를 처리한 자 9. 제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 10. 제59조제3호를 위반하여 다른 사람의 개인정보를 이용, 훼손, 멸실, 변경, 위조 또는 유출한 자

	제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 1. 제25조제5항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자 2. 현행과 같음 3. 현행과 같음 **제73조(벌칙)** 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. 1. 제36조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자 2. 제37조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 처리를 정지하지 아니하고 개인정보를 계속 이용하거나 제3자에게 제공한 자 3. 국내외에서 정당한 이유 없이 제39조의4에 따른 비밀유지명령을 위반한 자 4. 제63조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 자료제출 요구에 대하여 법 위반사항을 은폐 또는 축소할 목적으로 자료제출을 거부하거나 거짓의 자료를 제출한 자 5. 제63조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 출입·검사 시 자료의 은닉·폐기, 접근 거부 또는 위조·변조 등을 통하여 조사를 거부·방해 또는 기피한 자 ② 제1항제3호의 죄는 비밀유지명령을 신청한 자의 고소가 없으면 공소를 제기할 수 없다.

3. 개정내용 해설

□ 과징금 제도를 강화하면서 과도한 형벌 규정을 정비하였는데,

○ 안전조치 불이행으로 인한 개인정보 유출, 정보통신서비스 제공자 특례에 적용되던 동의 없는 개인정보 수집 위반·14세 미만 아동 법정대리인 동의 확인 의무 위반(동의의무 위반은 형벌 유지)·파기 의무 위반 등의 과도한 형벌 규정은 삭제하였고,

○ 정보통신서비스 제공자 특례에는 형벌 수준이 높던 정보주체의 정정·삭제 요구 미조치 후 이용·제공 관련 형벌 규정은 일반규정의 형량에 맞게 일원화하였다.

※ 5년 이하 징역 또는 5천만원 이하 벌금 → 2년 이하 징역 또는 2천만원 이하 벌금

□ 개인정보 처리를 위탁받아 처리하는 수탁자의 위반행위에 대하여도 개인정보처리자와 동일하게 제재할 수 있도록 명문화하였으며,

○ 개인정보취급자가 업무상 알게 된 개인정보를 사적으로 이용하는 것을 금지하고 위반 시 형사 처벌(5년 이하 징역 또는 5천만원 이하 벌금)이 가능하도록 하였으며, 법 제63조제1항 및 제2항에 따른 조사를 거부하거나 방해 또는 기피한 자에 대한 형사 처벌(2년 이하 징역 또는 2천만원 이하 벌금) 규정도 마련하였다.

4 과태료(법 제75조)

1. 개정 개요

□ 과징금 제도 개선으로 중대한 위반행위는 과징금으로 전환하고, 과태료 면제 요건 신설 등을 통해 경직적으로 운영되던 과태료 제도를 합리적으로 개선하였다.

○ CCTV 안내판 미설치, 손해배상의 보장 등 위반행위에 대해서는 먼저 시정조치 명령을 한 후 시정조치 명령 불이행 시 과태료를 부과하는 체제로 개편하였다.

2. 법령

법률	**제75조(과태료)** ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다. 1. 제25조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기를 설치·운영한 자 2. 제25조의2제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 자 ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다. 1. 제16조제3항·제22조제5항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 재화 또는 서비스의 제공을 거부한 자 2. 제20조제1항·제2항을 위반하여 정보주체에게 같은 조 제1항 각 호의 사실을 알리지 아니한 자 3. 제20조의2제1항을 위반하여 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하지 아니한 자 4. 제21조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 아니한 자 5. 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자 6. 제23조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 알리지 아니한 자 7. 제24조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 주민등록번호를 처리한 자 8. 제24조의2제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 암호화 조치를 하지 아니한 자 9. 제24조의2제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자 10. 제25조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기를 설치·운영한 자 11. 제25조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 자 12. 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자

	13. 제28조의5제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 아니하거나 이를 회수·파기하지 아니한 자 14. 제28조의8제4항(제26조제8항 및 제28조의11에 따라 준용되는 경우를 포함한다)을 위반하여 보호조치를 하지 아니한 자 15. 제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자 16. 제33조제1항을 위반하여 영향평가를 하지 아니하거나 그 결과를 보호위원회에 제출하지 아니한 자 17. 제34조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자 18. 제34조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하지 아니한 자 19. 제35조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 열람을 제한하거나 거절한 자 20. 제35조의3제1항에 따른 지정을 받지 아니하고 같은 항 제2호의 업무를 수행한 자 21. 제35조의3제3항을 위반한 자 22. 제36조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자 23. 제37조제3항 또는 제5항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 파기 등 필요한 조치를 하지 아니한 자 24. 제37조의2제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정당한 사유 없이 정보주체의 요구에 따르지 아니한 자 25. 제63조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자 26. 제63조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 출입·검사를 거부·방해 또는 기피한 자 27. 제64조제1항에 따른 시정조치 명령에 따르지 아니한 자 ③ 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다. 1. 제26조제6항을 위반하여 위탁자의 동의를 받지 아니하고 제3자에게 다시 위탁한 자 2. 제31조의2제1항을 위반하여 국내대리인을 지정하지 아니한 자 ④ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다. 1. 제11조의2제2항을 위반하여 정당한 사유 없이 자료를 제출하지 아니하거나 거짓으로 제출한 자 2. 제21조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자 3. 제22조제1항부터 제3항까지(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 동의를 받은 자 4. 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서로 하지 아니한 자 5. 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자 6. 제27조제1항·제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자 7. 제28조의4제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 관련 기록을 작성하여 보관하지 아니한 자 8. 제30조제1항 또는 제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리 방침을 정하지 아니하거나 이를 공개하지 아니한 자 9. 제31조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 아니한 자

	10. 제35조제3항・제4항, 제36조제2항・제4항 또는 제37조제4항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자 11. 제45조제1항에 따른 자료를 정당한 사유 없이 제출하지 아니하거나 거짓으로 제출한 자 12. 제45조제2항에 따른 출입・조사・열람을 정당한 사유 없이 거부・방해 또는 기피한 자 ⑤ 제1항부터 제4항까지의 규정에 따른 과태료는 대통령령으로 정하는 바에 따라 보호위원회가 부과・징수한다. 이 경우 보호위원회는 위반행위의 정도·동기·결과, 개인정보처리자의 규모 등을 고려하여 과태료를 감경하거나 면제할 수 있다.
시행령	**제63조(과태료의 부과기준)** 법 제75조에 따른 과태료의 부과기준은 별표 2와 같다. **[별표 2] 과태료의 부과기준(제63조 관련)** 1. 일반기준 가. 위반행위의 횟수에 따른 과태료의 가중된 부과기준은 최근 3년간 같은 위반행위로 과태료 부과처분을 받은 경우에 적용한다. 이 경우 기간의 계산은 위반행위에 대하여 과태료 부과처분을 받은 날과 그 처분 후 다시 같은 위반행위를 하여 적발된 날을 기준으로 한다. 나. 가목에 따라 가중된 부과처분을 하는 경우 가중처분의 적용 차수는 그 위반행위 전 부과처분 차수(가목에 따른 기간 내에 과태료 부과처분이 둘 이상 있었던 경우에는 높은 차수를 말한다)의 다음 차수로 한다. 다. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료 금액을 줄이거나 면제할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자에 대해서는 그렇지 않다. 1) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우 2) 위반의 내용・정도가 경미하다고 인정되는 경우 3) 위반행위자가 법 위반상태를 시정하거나 해소하기 위하여 노력한 것이 인정되는 경우 4) 위반행위자가 「중소기업기본법」 제2조에 따른 중소기업자인 경우 등 위반행위자의 업무 형태 및 규모에 비해 과중하다고 인정되는 경우 5) 위반행위자가 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치를 이행한 경우 6) 위반행위자가 개인정보 보호 인증을 받거나, 자율적인 보호 활동을 하는 등 개인정보 보호를 위하여 노력한 것이 인정되는 경우 7) 위반행위자가 위반행위 사실을 자진신고한 경우 8) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 줄이거나 면제할 필요가 있다고 인정되는 경우 라. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료의 2분의 1 범위에서 그 금액을 늘려 부과할 수 있다. 다만, 늘려 부과하는 경우에도 법 제75조제1항부터 제4항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다. 1) 위반의 내용・정도가 중대하여 정보주체 등에게 미치는 피해가 크다고 인정되는 경우 <삭 제> 2) 그 밖에 위반행위의 정도・기간, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 늘릴 필요가 있다고 인정되는 경우 2. 개별기준(생략)

3. 개정내용 해설

□ 중대한 위반행위는 과징금으로 전환하는 등 과태료 조항을 합리적으로 정비하였으며, 주요 내용은 다음의 표와 같다.

구분			내용	과태료 상한
§75 (과태료)	삭제	과징금 전환	개인정보 수집 위반(§15①)	-
			법정대리인 동의 위반(종전법 §22⑥→현행법 §22의2①)	-
			국외 이전 처리위탁·보관 미공개(종전법 §39조의12②단서→현행법 §28의8①)	-
			개인정보 동의 사항 고지 위반(§15②, §17②, §18③)	-
			손해배상 보장 불이행(종전법 §39의9①→현행법§39의7①)	-
			CCTV 안내판 미설치(§25④)	-
	특례 정비		서비스 제공 거부, 이용내역 통지, 파기(1천만원), 국외 이전 시 보호보치, 동의 철회, 국내대리인 지정(2천만원), 유출 통지·신고	3천만원
	신설		이동형 영상정보처리기기 촬영 위반(탈의실 5천만원, 공개된 장소 3천만원)	5/3천만원
			민감정보 공개 가능성 고지 위반	3천만원
			업무위탁에 따른 개인정보 처리 제한 위반	3천만원
			개인정보 영향평가 미실시	3천만원
			개인정보관리 전문기관 미지정 / 금지행위 위반	3천만원
			자동화된 결정에 대한 정보주체의 권리 행사 위반	3천만원
			개인정보 처리 재위탁 위반	2천만원
			개인정보 보호수준 평가 제출 위반	1천만원
			분쟁조정 자료제출, 검사 거부(§45①·②)	1천만원
	상향		조사 자료제출, 검사 거부(§63①·②): 1천만원 → 3천만원	3천만원

□ 과태료 부과 시 위반행위의 정도·동기·결과, 개인정보처리자의 규모 등을 고려하여 과태료를 감경하거나 면제할 수 있는 근거를 마련하였고, 가중·감경 고려사항을 정비하였다.

구분	가중	감경
비율	50% 이내	(종전) 50% 이내 → (개정) 50% 초과 및 면제 가능
고려 사항	(현행 유지) △위반 중대 (변경) △그 밖에 위반 정도 등 고려 → △그 밖에 위반 정도·기간 등 고려	(현행 유지) △사소한 부주의·오류, △위반 경미, △자진 시정 (변경) △중소기업 → 중소기업 외 업무·규모 고려 추가 (신설) △피해 회복, △자진신고, △자율보호

□ 보호위원회는 개인정보 보호법 개정에 따른 후속 조치로 「개인정보 보호법 위반에 대한 과태료 부과기준」 지침 개정(2023.9.15. 시행)을 통해 과태료 면제 규정 신설에 따른 요건 구체화, 과태료 감경 상한 확대, 과태료 가중·감경 사유의 종합적 고려 등 시행에 필요한 사항을 규정하였다.

4. 개인정보처리자 유의사항

□ 법 시행(2023.9.15.) 이전, 개인정보의 수집·이용(종전 법 §15①), 법정대리인의 동의(종전 법 §22⑥), 국외 이전 처리위탁·보관시 처리방침 공개 등(종전 법 §39조의12②단서), 개인정보 동의 사항 고지(종전 법 §15②, §17②, §18③) 의무를 위반한 경우에는 법 개정으로 과태료 규정이 삭제되었더라도 법 시행 전에 종료된 위반행위에 대하여는 개정된 규정에도 불구하고 종전의 규정이 적용되어 과태료 부과 대상에 해당한다.

※ 개인정보 보호법 시행령 부칙 제2조(과태료 부과에 관한 경과조치)

□ 법 시행(2023.9.15.) 이후, 개인정보 동의 사항 고지 의무(§15②, §17②, §18③)를 위반한 경우에는 과태료 규정이 삭제되었으나, 동의 사항에 대한 고지가 법 제22조 및 영 제17조를 위반하여 정보주체가 명확하게 인지할 수 있도록 알린 경우에 해당하지 않을 경우에는 동의 의무(§15①, §17①, §18①·②) 위반으로 법 제64조의2에 따라 과징금 부과 대상이 될 수 있으므로 유의해야 한다.

※ 해당 의무 위반사항이 경미한 경우에는 시정조치 명령이 가능하고, 시정조치 명령을 불이행한 경우 3천만원 이하 과태료가 부과될 수 있음

5. 제재 규정

□ 납부기한까지 과태료를 납부하지 아니한 때에는 납부기한을 경과한 날부터 체납된 과태료의 3%에 상당하는 가산금을 징수한다. 체납된 과태료를 납부하지 아니한 때에는 납부기한이 경과한 날부터 매 1개월이 경과할 때마다 체납된 과태료의 1.2%에 상당하는 가산금(중가산금)을 가산금에 가산하여 징수한다. 중가산금 기간은 60개월을 초과하지 못한다.

○ 그 밖에 일정 요건에 해당하는 경우 사업의 정지 또는 허가등의 취소, 감치를 할 수 있다.

6. 질의 응답

□ 법 시행 전 위반행위를 하였으나, 과태료 규정이 삭제된 경우에는 과태료가 부과되지 않는 것인지(법 시행 전 과태료 부과처분을 받은 경우에는 과태료 징수가 면제되는 것인지)?

⇨ (과태료 미부과되는 위반행위) CCTV 안내판 미설치, 손해배상 보장 불이행에 대해서는 과태료가 부과되지 않음(이미 과태료가 부과된 경우에는 징수·집행이 면제됨)

(과태료 부과되는 위반행위) 개인정보 수집, 법정대리인 동의, 국외 이전 처리위탁·보관 미공개, 개인정보 동의 항목 고지 위반에 대해서는 종전의 규정을 적용하여 과태료를 부과하며, 과징금은 부과되지 않음

※ 개인정보 보호법 시행령 부칙 제2조(과태료 부과에 관한 경과조치)

□ 법 시행 전 위반행위에 대해서도 법 제75조제5항에 따른 과태료 면제가 가능한지?

⇨ 법 제75조제5항에 따른 과태료 면제 요건 신설에 따라 법 시행 전 위반행위에 대해서도 법 제75조제5항에 따른 과태료 면제가 가능함

※ 개인정보 보호법 제75조 ⑤ (전단 생략) 이 경우 보호위원회는 위반행위의 정도・동기・결과, 개인정보처리자의 규모 등을 고려하여 과태료를 감경하거나 면제할 수 있다.

※ 질서위반행위규제법 제3조(법 적용의 시간적 범위) ② 질서위반행위 후 법률이 변경되어 그 행위가 질서위반행위에 해당하지 아니하게 되거나 과태료가 변경되기 전의 법률보다 가볍게 된 때에는 법률에 특별한 규정이 없는 한 변경된 법률을 적용한다.

참고 개인정보 보호법 위반에 대한 과태료 부과기준('23.9.15. 시행)

제1조(목적) 이 지침은 「개인정보 보호법」(이하 "법"이라 한다) 제75조, 같은 법 시행령(이하 "영"이라 한다) 제63조 및 [별표 2]에 규정된 위반행위에 대한 과태료 부과의 절차와 기준에 관하여 필요한 사항을 정함을 목적으로 한다.

제2조(정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "위반행위"란 법을 위반하여 법 제75조의 과태료 부과 대상이 되는 행위를 말한다.

2. "기준금액"이란 영 [별표 2] 개별기준의 각 목별 위반행위에 대하여 위반횟수별로 규정된 과태료 금액을 말한다.

3. "조정금액"이란 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 각 위반행위별 기준금액에 제6조 또는 제7조에 따라 감경 또는 가중하는 금액을 말한다.

4. "과태료 부과금액"이란 기준금액에 조정금액을 가산 또는 차감하여 최종적으로 위반행위자에게 부과하는 과태료 금액을 말한다.

제3조(과태료의 면제) ① 위반행위가 다음 각 호의 어느 하나에 해당하는 경우에는 과태료를 부과하지 아니한다.

1. 「질서위반행위규제법」 제7조에서 정한 바와 같이 당사자의 고의 또는 과실이 없는 경우

2. 「질서위반행위규제법」 제8조에서 정한 바와 같이 당사자의 질의에 대한 담당 공무원의 서면회신이나 행정지도 기타 공적인 견해표명 등에 의하여 자신의 행위가 위법하지 아니한 것으로 오인하고 행한 행위로서 그 오인에 정당한 사유가 있는 경우

3. 「질서위반행위규제법」 제9조에서 정한 바와 같이 14세가 되지 아니한 자의 위반행위

4. 「질서위반행위규제법」 제10조제1항에서 정한 바와 같이 심신(心神)장애로 인하여 행위의 옳고 그름을 판단할 능력이 없거나 그 판단에 따른 행위를 할 능력이 없는 자의 위반행위. 다만 스스로 심신장애 상태를 일으켜 질서위반행위를 한 자에 대하여는 그렇지 않다.

② 다음 각 호의 어느 하나에 해당하는 경우에는 과태료를 부과하지 않을 수 있다. 다만, 본문에 따라 과태료 부과처분을 받지 않은 자가 그 결정이 있은 날부터 3년 이내에 같은 위반행위를 하는 경우에는 그렇지 않다.

1. 위반행위의 내용·정도가 경미하거나 사소한 부주의나 오류로 인한 위반행위인 경우

2. 정보주체에게 피해가 발생하지 아니하였거나 경미한 경우로서 위반행위를 시정한 경우

3. 위반행위자가 「소상공인기본법」 제2조에 따른 소상공인인 경우 등인 경우로서 부과하고자 하는 과태료 금액이 위반행위자의 현실적인 부담능력을 벗어나 과중하다고 인정되는 경우

4. 제1호부터 제3호까지에 준하는 사유가 있어 과태료 부과의 면제가 불가피하다고 인정되는 경우

제4조(과태료의 부과기준) ① 과태료 부과금액은 영 [별표 2]에 따른 각 위반행위별 기준금액에 조정금액을 가산하거나 차감하여 결정한다.

o 과태료 부과금액 = 기준금액 ± 조정금액

② 조정금액은 제6조와 제7조에서 정한 감경 또는 가중 사유가 인정되는 경우 다음과 같이 산정한다.

o 조정금액 = 가중금액 - 감경금액 o 가중금액 = 위반행위별 기준금액 × 가중비율의 합계 o 감경금액 = 위반행위별 기준금액 × 감경비율의 합계

③ 하나의 행위가 2개 이상의 위반행위에 해당하는 경우에는 각 위반행위에서 정한 과태료 중 가장 중한 과태료를 부과한다.

④ 2개 이상의 위반행위가 경합하는 경우에는 각 위반행위에 대하여 정한 과태료를 각각 부과한다.

제5조(기준금액의 산정) 최근 3년간 같은 위반행위로 과태료 처분을 받았거나 「비송사건절차법」에 따른 과태료 재판 결정을 받은 위반횟수를 확인하고 위반횟수별 해당 과태료 금액을 기준금액으로 한다. 이 경우 기준금액을 산정할 때 영 [별표 2] 제1호 가목·나목에 따른 가중된 부과처분의 적용 순서도 및 예시는 [별표 1]과 같다.

제6조(과태료의 감경) ① 개인정보 보호위원회(이하 "보호위원회"라 한다)는 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 2]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다. 다만, 과태료를 체납하고 있는 경우는 제외한다.

② [별표 2]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 감경하되, 제2호 1) 및 2)에 해당하는 사유가 각 2개 이상 해당되는 경우에는 기준금액의 100분의 50을 초과할 수 없고, 최종 합산 결과 기준금액의 100분의 90을 초과할 수 없다.

제7조(과태료의 가중) ① 보호위원회는 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 3]의 가중기준에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.

② [별표 3]의 각 기준에 따른 과태료 가중 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 가중하되, 기준금액의 100분의 50을 초과할 수 없다.

제8조(과태료 부과금액의 결정) 위반행위별 과태료 금액이 법 제75조제1항부터 제4항까지의 규정에 따른 과태료 금액의 상한을 넘는 경우에는 과태료 금액의 상한을 과태료 부과금액으로 한다.

제9조(자진납부자에 대한 과태료 감경) 보호위원회로부터 과태료 고지서를 송달받은 날부터 14일 이내에 과태료를 납부하는 자에 대해서는 「질서위반행위규제법」 제18조 및 같은 법 시행령 제5조를 준용하여 해당 과태료 부과금액의 100분의 20을 감경한다.

부칙 <신설, 2021. 1. 27>

제1조(시행일) 이 지침은 2021년 1월 27일부터 시행한다.

제2조(경과규정) 2020년 8월 5일 이후 발생한 위반행위에 대한 과태료 부과 시점부터 이 지침을 적용한다.

부칙 <일부개정, 2023. 3. 8.>

이 지침은 2023년 3월 8일부터 시행한다.

부칙 <일부개정, 2023. 9. 11.>

제1조(시행일) 이 지침은 2023년 9월 15일부터 시행한다. 다만, [별표 2] 제2호 2) (1) 개인정보 보호 활동 2.의 개정규정은 2024년 3월 15일부터 시행한다.

제2조(과태료 부과기준에 관한 경과조치 등) ① 과태료 부과기준은 이 지침 시행 전에 종료된 위반행위에 대해서도 적용한다.

② 이 지침 시행 전에 종료된 위반행위에 대한 과태료의 감경기준(위반 정도, 사업 규모, 개인정보 보호 인증, 위탁사로서 수탁사(협력사) 등에 대한 지원·협력을 위해 적극 노력한 경우, 조사 협조·자진시정 등 및 기타에 한한다)은 [별표 2] 제2호의 개정규정에도 불구하고 종전의 [별표 1]에 따른다.

③ 이 지침 시행 전에 종료된 위반행위에 대한 과태료의 가중기준(조사 방해, 위반 주도에 한한다) 및 가중비율(위반의 정도에 한한다)은 [별표 3] 제2호의 개정규정에도 불구하고 종전의 [별표 2] 제2호에 따른다.

[별표 1] 가중처분 적용 순서도 및 예시(제5조 관련)

[별표 2]

과태료의 감경기준(제6조 관련)

1. 위반행위자에 대하여 제2호에서 정한 감경사유가 인정되는 경우에는 각 감경사유별 감경비율의 범위

내에서 감경할 수 있다.

2. 과태료의 감경기준은 다음과 같다.

1) 당사자 환경 및 위반 정도 등 : 기준금액의 50% 이내

기준	감경사유	감경비율
당사자 환경 * 근거: 「질서위반행위규제법 시행령」 제2조의2	1.「국민기초생활 보장법」 제2조에 따른 수급자	기준금액의 50% 이내
	2.「한부모가족 지원법」 제5조 및 제5조의2제2항·제3항에 따른 보호대상자	
	3.「장애인복지법」 제2조에 따른 장애인 중 장애의 정도가 심한 장애인	
	4.「국가유공자 등 예우 및 지원에 관한 법률」 제6조의4에 따른 1급부터 3급까지의 상이등급 판정을 받은 사람	
	5. 14세 이상 19세 미만의 미성년자	
	6.「질서위반행위규제법」 제10조제2항에 따른 심신장애자 * 다만 스스로 심신장애 상태를 일으켜 위반행위를 한 자는 제외한다.	
	※ 상기 1.~5. 항목에 해당하여 감경 시「질서위반행위규제법」 제18조에 따른 자진납부자 감경을 제외하고 하단 사유로 추가 감경 불가	
위반 정도	위반행위의 내용·정도가 경미하다고 인정되거나 사소한 부주의나 오류로 인한 위반행위로 인정되거나 정보주체에게 피해가 발생하지 아니하였거나 경미한 경우로서 면제에 이르지 아니한 경우	기준금액의 30% 이내
개인정보처리자의 업무 형태 및 규모	1. 위반행위자가 비영리법인, 비영리단체 등인 경우로서 무보수성, 공익성, 비영리성 등을 고려할 때 과중하다고 인정되는 경우	기준금액의 30% 이내
	2.「중소기업기본법」 제2조에 따른 소기업(小企業)인 경우	기준금액의 30% 이내
	3.「중소기업기본법」 제2조에 따른 중기업(中企業)인 경우	기준금액의 15% 이내

2) 개인정보 보호 노력, 조사 협조·자진 시정 등 : 기준금액의 50% 이내

(1) 개인정보 보호를 위한 노력 정도

기준	감경사유	감경비율
개인정보 보호 인증	1. 위반행위자가 법 제32조의2에 따른 개인정보 보호 인증(ISMS-P)을 받은 경우 * 유효한 PIMS 인증 등을 포함한다.	기준금액의 40% 이내
	2. 위반행위자가「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제2항 각 호의 어느 하나에 해당하지 아니하는 자로서 정보보호 관리체계 인증(ISMS)을 받은 경우	기준금액의 20% 이내
	3. 개인정보 보호 관련 국제인증(ISO27701)을 받은 경우	기준금액의 20% 이내

	4. 개인정보 보호 관련 국제인증(ISO27001, BS10012)을 받은 경우	기준금액의 20% 이내
	5. 위반행위자가 민간자율의 개인정보 보호 마크 인증(ePRIVACY PLUS, PRIVACY 등)을 받은 경우	기준금액의 10% 이내
	※ 상기 1.~5. 항목은 인증범위 내에 위반행위가 발생한 개인정보처리시스템이 있는 경우에만 적용한다. ※ 상기 1.~5. 항목 중 두 가지 이상에 해당하는 경우에는 가장 높은 감경비율을 적용한다.	
자율규제 규약 등	개인정보 보호 자율규제 규약을 이행하는 등 개인정보 보호 활동을 성실히 수행한 것으로 확인된 경우	기준금액의 40% 이내
개인정보 보호 활동	1. 개인정보 처리방침의 평가의 결과가 상위 등급인 경우	기준금액의 10% 이내
	2. 개인정보 보호수준 평가의 결과가 상위 등급인 경우	기준금액의 10% 이내
	3. 개인정보 영향평가를 하는 등 개인정보 보호 활동을 성실히 수행한 것으로 확인된 경우 * 다만, 법 제33조제1항에 따라 개인정보 영향평가를 해야 하는 경우는 제외	기준금액의 10% 이내
	4. 개인정보 보호책임자 및 개인정보취급자의 업무에 요구되는 전문적인 교육훈련을 정기적으로 성실히 수행하거나 표창을 받는 등 개인정보 보호를 위한 노력이 상당히 있는 경우	기준금액의 5% 이내
	※ 상기 1.~2. 항목은 가장 최근에 시행한 평가 결과를 반영하고, 상기 2.~3. 항목은 평가범위 내에 위반행위가 발생한 개인정보처리시스템이 있는 경우에만 적용한다. ※ 상기 1.~4. 항목 중 두 가지 이상에 해당하는 경우에는 가장 높은 감경비율을 적용한다.	

※ 비고 : “민간자율의 개인정보 보호 마크 인증(ePRIVACY PLUS, PRIVACY 등)”이란 개인정보를 수집·처리하는 기관 등을 대상으로 개인정보 보호 적정성 등 50개 이상의 심사항목에 따라 심사·인증하는 제도(OPA 등 법상 민간자율단체 부여)

(2) 조사 협조, 자진 시정 등

기준	감경사유	감경비율
조사 협조	보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 20% 이내
자진 시정 등	1. 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 20% 이내
	2. 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완	기준금액의

	료하지는 못하였으나 시정 중에 있는 것으로 인정되는 경우	10% 이내
피해 회복 · 피해 확산 방지	개인정보 분쟁조정, 민사조정 등을 통해 정보주체에게 발생한 피해에 대한 원상회복, 손해배상 또는 이에 상당하는 필요한 피해구제 조치를 적극적으로 이행한 경우 * 다만, 법 제39조의7에 따른 손해배상책임 이행을 위한 보험 등 가입은 제외	기준금액의 30% 이내
자진 신고	위반행위 사실을 자진신고 한 경우 * 다만, 법 제34조제3항 전단에 따른 신고는 제외	기준금액의 20% 이내

[별표 3]

과태료의 가중기준(제7조 관련)

1. 위반행위자에 대하여 제2호에서 정한 가중사유가 인정되는 경우에는 각 가중사유별 가중비율의 범위 내에서 가중할 수 있다.

2. 과태료의 가중기준은 다음과 같다.

기준	가중사유	가중비율
위반의 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우	기준금액의 30% 이내
	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 15% 이내
위반 기간	1. 법 위반 상태의 기간이 2년을 초과하는 경우	기준금액의 30% 이내
	2 법 위반 상태의 기간이 1년 초과 2년 이내인 경우	기준금액의 15% 이내
조사 방해	위반행위자 및 그 소속 임직원이 법 제63조제1항 및 제2항에 따른 물품·서류의 제출요구 또는 검사를 거부하거나 증거인멸, 은폐, 조작, 허위의 정보제공 등의 방법으로 조사를 방해하거나, 관련 정보주체 등에게 허위로 진술하도록 요청한 경우 * 다만, 법 제63조제1항·제2항에 따른 물품·서류의 제출요구 또는 검사를 거부·방해 또는 기피한 행위(법 제75조제2항제25호·제26호)로 과태료를 부과 받은 경우에는 가중하지 아니한다.	기준금액의 50% 이내
위반 주도	다수의 위반행위자가 관련된 상황에서 위반행위를 주도하거나 선도한 경우	기준금액의 20% 이내

3. 제2호 가중사유의 위반행위별 각 목의 세부기준은 아래와 같다.

위반행위별	세부기준
영 별표2 제2호 아목	법 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치로서,

	<개인정보처리자의 경우> 가. 영 제30조제1항제1호에 따라 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 및 점검을 하지 않은 경우 나. 영 제30조제1항제2호에 따라 개인정보에 대한 접근 권한을 제한하기 위한 조치를 하지 않은 경우 다. 영 제30조제1항제3호에 따라 개인정보에 대한 접근을 통제하기 위한 조치를 하지 않은 경우 라. 영 제30조제1항제4호에 따라 개인정보를 안전하게 저장·전송하는데 필요한 조치를 하지 않은 경우 마. 영 제30조제1항제5호에 따라 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치를 하지 않은 경우 바. 영 제30조제1항제6호에 따라 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터 바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치를 하지 않은 경우 사. 영 제30조제1항제7호에 따라 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치를 하지 않은 경우 아. 영 제30조제1항제8호에 따라 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치를 하지 않은 경우 자. 영 제29조의5제1항제2호에 따라 가명정보와 추가정보를 분리 보관하지 않은 경우 차. 영 제29조의5제1항제3호에 따라 가명정보와 추가정보에 대한 접근 권한을 분리하지 않은 경우 **<공공시스템 운영기관 등의 경우>** 가. 영 제30조의2제1항제1호에 따라 내부 관리계획에 공공시스템별로 작성한 안전성 확보 조치를 포함하지 않은 경우 나. 영 제30조의2제1항제2호에 따라 공공시스템이용기관이 정당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치를 하지 않은 경우

	다. 영 제30조의2제1항제3호에 따라 개인정보에 대한 불법적인 접근 및 침해사고 방지를 위한 공공시스템 접속기록의 저장·분석·점검·관리 등의 조치를 하지 않은 경우 라. 영 제30조의2제2항에 따라 공공시스템운영기관 및 공공시스템이용기관이 정당한 권한 없이 또는 허용된 권한을 초과하여 개인정보에 접근한 사실이 확인되는 경우에도, 지체 없이 정보주체에게 해당 사실과 피해 예방 등을 위해 필요한 사항을 통지하지 않은 경우 마. 영 제30조의2제3항에 따라 공공시스템운영기관(공공시스템을 개발하여 배포하는 기관이 따로 있는 경우에는 그 공공기관을 포함한다)이 해당 공공시스템의 규모와 특성, 해당 공공시스템이용기관의 수 등을 고려하여 개인정보의 안전한 관리에 관련된 업무를 전담하는 부서를 지정하여 운영하거나 전담인력을 배치하지 않은 경우 바. 영 제30조의2제4항에 따라 공공시스템운영기관(공공시스템을 개발하여 배포하는 기관이 따로 있는 경우에는 그 공공기관을 포함한다)이 공공시스템별로 해당 공공시스템을 총괄하여 관리하는 부서의 장을 관리책임자로 지정(해당 공공시스템을 총괄하여 관리하는 부서가 없을 때에는 업무 관련성 및 수행능력 등을 고려하여 해당 공공시스템운영기관의 관련 부서의 장 중에서 지정) 하지 않은 경우 사. 영 제30조의2제5항에 따라 공공시스템운영기관이 공공시스템에 대한 안전성 확보 조치 이행상황 점검 및 개선에 관한 사항을 협의하기 위하여 공공시스템운영협의회를 설치·운영하지 않은 경우
영 별표2 제2호 저목	가. 법 제28조의5제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 아니한 경우 나. 법 제28조의5제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이를 회수·파기하지 아니한 경우

※ 참고 : 법 및 영 등 개정으로 제3호의 위반행위별 각 목의 세부기준이 변경되는 경우에는 개정된 법령을 따른다.

참고 **개인정보 보호위원회의 조사 및 처분에 관한 규정('23.10.16. 시행)**

제1장 총칙

제1조(목적) 이 규정은 「개인정보 보호법」(이하 "법"이라 한다) 제63조제5항에 따라, 개인정보 보호위원회(이하 "보호위원회"라 한다)가 법 제34조, 제62조, 제63조, 제63조의2 및 제68조, 같은 법 시행령(이하 "영"이라 한다) 제40조, 제60조 및 제62조, 「신용정보의 이용 및 보호에 관한 법률」(이하 "신용정보법"이라 한다) 제39조의4 및 제45조의3, 같은 법 시행령 제34조의2 및 제36조의4에 따라 실시하는 조사 및 사전 실태점검(이하 "조사등"이라 한다)의 절차와 방법, 그 결과에 따른 처분 및 기타 필요한 사항을 정함으로써 조사등의 공정성과 투명성 및 효율성을 확보하는 것을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "조사관"이란 법, 신용정보법(이하 "개인정보 보호 법령"이라 한다) 및 이 규정에 따라 조사등 업무를 수행하는 보호위원회 소속 공무원을 말한다.
2. "위반행위"란 다음 각 목의 규정을 위반하는 행위를 말한다.
   가. 법 제15조부터 제28조의5까지, 제28조의8, 제28조의9, 제28조의11부터 제30조까지, 제31조부터 제35조의3까지, 제36조부터 제38조까지 및 제39조의7
   나. 신용정보법 제15조, 제17조, 제19조, 제20조의2, 제32조, 제33조, 제34조, 제36조, 제37조, 제38조, 제38조의3, 제39조의4, 제40조의2 및 제42조
3. "조사대상자"란 개인정보 보호 법령 및 이 규정에 따라 보호위원회의 조사등을 받는 법 제2조제5호에 따른 개인정보처리자(법 제26조제2항에 따른 수탁자를 포함한다. 이하 같다) 및 신용정보법 제45조의3제1항에 따른 상거래기업 및 법인(같은 법 제17조제2항에 따른 수탁자를 포함한다. 이하 같다)을 말한다.

제3조(다른 규정과의 관계) 이 규정에서 특별히 규정하지 않은 사항은 「행정기본법」, 「행정절차법」, 「행정조사기본법」에서 정하는 바에 따른다.

제2장 조사

제1절 조사의 사전검토 등

제4조(위반행위의 신고 등) ① 누구든지 위반행위가 있다고 인정할 때에는 다음 각 호의 사항을 기재한 신고서와 위반행위를 소명할 만한 자료를 보호위원회에 제출할 수 있다.

1. 신고인의 성명(법인인 경우에는 법인의 명칭 및 대표자의 성명), 연락처
2. 피신고인의 성명(법인인 경우에는 법인의 명칭 및 대표자의 성명), 연락처
3. 위반행위의 내용

② 보호위원회는 개인정보 보호 법령 및 이 규정에 따라 신고서 등을 제출받은 때에는 신고서 등의 기재사항을 검토하고 미비한 부분이 있는 경우에는 7일 이내의 기간을 정하여 신고인에게 보완을 요구할 수 있다. 이 경우 보완을 요구한 날부터 보완이 완료된 날까지의 기간은 제5조제2항에 따른 기간 산정 시 산입하지 아니한다.

③ 신고의 경험이 없는 자가 개인정보 보호 법령 및 이 규정에 따라 신고서 등을 제출할 때에는 보호위원회 또는 법 제34조제3항 전단 및 후단 또는 법 제62조에 따른 전문기관(이하 "전문기관"이라 한다)의 도움을 받을 수 있다.

제4조의2(자진신고) 법 제34조제3항 전단에도 불구하고 개인정보처리자는 위반행위 사실을 보호위원회에 자진신고할 수 있다.

제5조(사전검토 등) ① 보호위원회 직제에 따른 소관 국(이하 "해당 국"이라고 한다)의 국장(이하 "해당

국장"이라 한다)은 다음 각 호의 어느 하나의 경우에는 이를 담당할 조사관을 지정하여 조사착수에 필요한 사실관계의 확인 등 사전검토를 할 수 있다.

1. 제4조 등에 따른 신고(법 제34조제3항 전단 및 신용정보법 제39조의4제4항에 따른 유출 등의 신고(이하 "유출신고"라 한다), 법 제62조에 따른 침해 사실의 신고, 제4조의2에 따른 자진신고(이하 "자진신고"라 한다), 민원, 「공익신고자 보호법」에 따른 공익신고, 다른 기관이 이첩한 신고를 포함한다. 이하 같다)를 접수한 경우
2. 개인정보 유출 등 위반행위의 혐의 사실을 인지한 경우

② 조사관은 제4조 등에 따른 신고의 경우에는 사건을 지정받은 날부터 14일 이내에 해당 국장에게 조사착수 여부의 보고를 마쳐야 한다. 다만, 사실관계가 복잡한 사건의 경우에는 14일 이내로 기간을 연장할 수 있다.

③ 조사관은 사전검토를 위하여 필요한 경우에는 조사대상자에게 관련 자료나 물건의 제출을 요구할 수 있다. 이 경우 자료제출 요구에 관하여는 제9조를 준용한다.

제5조의2(조사를 개시하지 않는 경우) 해당 국장은 다음 각 호의 어느 하나의 경우에는 조사에 착수하지 않을 수 있다.

1. 신고인이 신고를 취하한 경우
2. 제4조제2항에 따른 보완 요구를 할 수 없는 경우 또는 보완 요구를 받고도 보완을 하지 않거나 보완 내용이 분명하지 않은 경우로서 조사착수가 불가능하다고 판단되는 경우
3. 이미 처리한 사건과 동일한 사건(조사대상자와 위반행위가 동일한 사건을 말한다)인 경우
4. 개인정보 보호 법령 적용 대상이 아니라고 인정되는 경우
5. 위반행위로 인정되지 않는 것이 명백한 경우
6. 피신고인에게 사망, 청산 또는 이에 준하는 사유가 발생함으로써 조사를 하기가 사실상 불가능하다고 인정되는 경우
7. 제1호부터 제6호까지에 준하는 경우

제2절 조사의 절차 및 방법

제6조(조사의 착수) 해당 국장은 제5조제1항 각 호의 어느 하나에 해당하는 경우로서 조사의 필요성이 인정되는 경우에는 조사에 착수하여야 한다. 이 경우 조사관은 사건의 개요, 조사방법 및 일정 등을 포함한 조사착수 보고서를 작성하여 해당 국장에게 보고하여야 한다.

제6조의2(사건의 등록 및 관리) ① 조사관은 제6조에 따라 조사에 착수하는 경우 해당 사건을 지체 없이 사건처리시스템에 등록하고, 사건번호 및 사건의 명칭을 부여하여 체계적으로 관리하여야 한다.

② 사건번호는 사건을 식별하여 효율적으로 관리하기 위해 다음 각 호의 순서에 따라 순차 기재하여 부여한다.

1. 조사 착수연도
2. 사건별 부호문자
3. 접수일련번호

③ 사건번호는 조사대상자, 위반행위의 동일성, 조사대상이 되는 분야 등을 기준으로 부여한다.

④ 사건의 명칭은 해당 사건의 내용을 알 수 있도록 정한다.

⑤ 사건은 계류 현황, 처리 완료 현황 및 지연 현황 등을 파악할 수 있도록 관리하여야 한다.

제7조(조사기간) ① 사건의 조사개시일은 제6조에 따른 조사착수 보고일로 한다. 다만, 제31조에 따라 전문기관에 조사를 위탁하는 경우에는 전문기관으로부터 조사결과 자료를 송부받은 날로 한다.

② 조사관은 조사개시일로부터 6개월(조사내용이 복잡하고 전문성이 요구되는 사건의 경우 12개월) 이내에 제15조제1항에 따른 조사결과 보고를 마쳐야 한다. 다만, 부득이한 사유로 조사기간의 연장이 필요한 경우에는 연장기간을 정하여 해당 국장에게 보고하여야 한다.

제7조의2(조사대상) 조사관은 조사대상자의 대표자, 임직원, 참고인 등에 대해서도 조사를 할 수 있다.

제8조(조사의 범위) 조사관은 제9조, 제10조 또는 제11조에 따라 조사대상자에게 통지하는 문서(전자문서를 포함한다. 이하 "조사공문"이라 한다)에 기재된 조사목적 범위 내에서 조사를 실시하여야 한다.

제8조의2(사건의 분리 및 병합) ① 해당 국장은 위반행위의 동일성이 인정되는 등 필요하다고 인정할 때에는 사건을 병합하거나 분리할 수 있다.

② 사건을 병합하는 경우의 조사기간은 조사기간이 가장 늦은 사건의 조사기간을 따르고, 사건을 분리하는 경우의 조사기간은 각 사건의 원래 조사기간을 따른다.

제8조의3(조사의 중지 등) ① 해당 국장은 다음 각 호의 어느 하나에 해당하는 경우에는 조사를 중지할 수 있다. 이 경우 조사를 중지한 날부터 조사가 재개된 날까지의 기간은 제7조에 따른 기간 산정 시 산입하지 아니한다.

1. 조사대상자의 부도, 휴업, 폐업, 도피, 소재불명, 연락두절 등의 경우
2. 수사기관의 수사나 법원의 재판 등의 결과가 조사 등을 위해 필요하나 그 결과에 상당한 시일이 소요되는 경우
3. 국내에 주소 또는 영업소가 없는 조사대상자를 조사하는 경우로서 조사를 하기가 현저히 곤란한 경우
4. 제1호부터 제3호까지에 준하는 경우

② 조사관은 제1항에 따라 조사를 중지하는 경우에는 조사중지 사유가 해소되었는지 여부를 점검 및 관리하여야 한다.

③ 해당 국장은 조사를 중지한 날부터 6개월이 경과한 후에도 그 사유가 해소되지 않은 경우에는 제15조의2제1항에 따른 조사종결을 할 수 있다. 이 경우 조사관이 조사결과 보고서를 작성할 때에는 "조사대상자에게 영업 재개 등의 조사 개시 사유가 발생한 때에는 재조사할 수 있다"는 문구를 명백히 기재하여야 한다.

제9조(자료제출 요구) ① 조사관은 사건의 조사를 위하여 필요한 경우에는 조사대상자에게 관련 자료나 물건의 제출을 요구할 수 있다.

② 제1항에 따른 자료나 물건의 제출을 요구할 때에는 다음 각 호의 사항이 기재된 조사공문으로 한다.

1. 제출요청사유
2. 자료를 제출할 자
3. 제출할 서류, 물건 등 자료
4. 제출기한과 장소
5. 제출방식
6. 자료제출 요청에 응하지 아니하는 경우 제재 내용

제10조(현장조사) ① 조사관은 사건의 조사를 위하여 필요한 경우에는 조사대상자의 사무소 또는 사업장(이하 "사무소등"이라 한다)에 출입하여 그 대표자, 대리인, 그 밖의 임직원 등(이하 "관계인"이라 한다)에게 진술을 요구하거나 관계인을 참관시킨 후 업무 상황, 장부·서류, 기타 자료나 물건을 조사하고, 해당 자료나 물건의 제출을 요구할 수 있다.

② 조사관은 제1항에 따른 현장조사를 개시하기 이전에 조사대상자에게 다음 각 호의 사항이 기재된 조사공문을 통지하여야 한다. 다만, 긴급한 경우나 사전통지를 하면 증거인멸 등으로 조사목적을 달성할 수 없다고 인정하는 경우에는 현장조사의 개시와 동시에 조사대상자에게 조사공문을 교부할 수 있다.

1. 조사목적
2. 조사기간

3. 조사내용
4. 협조사항
5. 조사를 거부·방해 또는 기피할 경우 소관 법률상의 제재 내용
6. 제1호부터 제4호까지의 범위를 벗어난 조사에 대해서는 거부할 수 있다는 내용
7. 조사단계에서 조사대상자가 보호위원회 또는 조사관에게 조사와 관련된 의견을 제시하거나 진술할 수 있다는 내용

③ 조사관이 제1항에 따라 조사대상자의 사무소등에 출입하고자 할 때에는 공무원증 및 조사공문 등 그 권한을 표시하는 증표를 제시하여야 한다.

④ 조사관은 제1항에 따른 현장조사를 하는 경우에는 조사장소, 조사기간, 조사내용, 제출한 자료나 물건의 목록, 조사관 및 관계인의 성명 등을 기재한 현장조사서를 작성하여야 한다.

⑤ 조사관은 제4항에 따라 작성한 현장조사서를 관계인에게 열람하여 기재 내용의 정확 여부를 확인하게 하고, 관계인과 함께 해당 현장조사서에 서명 또는 날인한다. 다만, 관계인이 서명 또는 날인을 거부하는 경우에는 그 사실을 현장조사서에 기재하여야 한다.

⑥ 조사관은 관계인이 제1항에 따른 사무소등에의 출입을 거부 또는 방해하거나 진술 또는 자료의 제출을 거부한 경우에는 그 사실을 기재한 확인서를 작성하고, 관계인과 함께 해당 확인서에 서명 또는 날인한다. 다만, 관계인이 서명 또는 날인을 거부하는 경우에는 그 사실을 확인서에 기재하여야 한다.

⑦ 조사관은 현장조사가 종료되면 조사대상자의 방어권이 보장될 수 있도록 현장조사 이후의 보호위원회의 사건처리절차에 대하여 조사대상자에게 관련 내용이 포함된 서면을 교부하거나 충분히 설명하여야 한다.

제11조(출석·진술 요구) ① 조사관은 사건의 조사를 위하여 필요한 경우에는 조사대상자에게 출석·진술을 요구할 수 있다.

② 제1항에 따른 출석·진술을 요구할 때에는 다음 각 호의 사항이 기재된 조사공문을 발송하여야 한다.

1. 출석요구의 취지
2. 출석 대상자
3. 출석일시 및 장소
4. 출석하여 진술하여야 하는 내용
5. 제출자료

제11조의2(조사 과정의 녹음·녹화) 조사관은 사건의 조사를 위해 필요한 경우에는 조사의 과정을 녹음하거나 녹화할 수 있다. 이 경우 녹음·녹화의 범위 등은 조사대상자와 협의하여 정하여야 한다.

제12조(공동조사 등) ① 보호위원회는 법 등 개인정보 보호와 관련된 법규의 위반행위로 인하여 중대한 개인정보 침해사고가 발생한 경우 신속하고 효과적인 대응을 위하여 법 제63조제3항에 따라 관계 기관의 장에게 협조를 요청할 수 있다.

② 제1항에 따라 협조를 요청받은 관계 기관의 장은 법 제63조제4항에 따라 특별한 사정이 없으면 이에 따라야 한다.

③ 관계 중앙행정기관은 소관 법률의 적용을 받는 개인정보처리자의 위반행위를 발견하거나 혐의가 있음을 알게 된 경우 보호위원회에 이를 알려야 한다.

제12조의2(제출기한의 연장 등) 조사대상자는 부득이한 사유로 자료제출(제16조의2에 따른 의견제출 등을 포함한다. 이하 같다)기한의 연장 및 현장조사, 출석 일시 등의 변경(이하 "제출기한의 연장 등"이라 한다)이 필요한 경우에는 제출기한이 경과하거나 해당 조사 등을 개시하기 전에 제출기한의 연장 등의 사유 및 내용을 보호위원회에 알려야 하며, 보호위원회는 조사목적을 달성할 수 있는 범위 안에서 제출기한의 연장 등을 허용할 수 있다.

제13조(변호인의 참여) ① 조사관은 조사대상자의 신청이 있는 경우 원칙적으로 조사대상자가 선임한 변호인을 조사 과정에 참여하게 하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 조사대상자의 변호인 참여 요청이 조사의 개시 및 진행을 지연시키거나 방해하는 것으로 판단되는 경우
2. 조사관의 승인 없이 조사에 개입하거나 모욕적인 언동 등을 행하는 경우
3. 조사대상자를 대신하여 답변하거나 특정한 답변 또는 진술 번복을 유도하는 경우
4. 신문내용을 촬영, 녹음, 기록하는 경우. 다만, 기록의 경우 조사대상자에 대한 법적 조언을 위해 변호인이 기억환기용으로 간략히 메모를 하는 것은 제외한다
5. 그 밖에 조사목적 달성을 현저하게 어렵게 하는 경우

② 제1항에도 불구하고, 증거인멸 우려 등의 사유로 조사의 긴급을 요하는 경우에는 조사대상자의 변호인 참여 요청과 관계없이 조사를 개시하고 진행할 수 있다.

제14조(비밀엄수 및 제출받은 자료의 사용 제한) ① 조사관은 조사가 진행 중인 사항은 물론 조사와 관련하여 알게 된 사실을 누설하여서는 아니된다.

② 제9조, 제10조, 제11조 또는 제16조의2에 따라 제출받은 자료와 조사를 통해 알게 된 정보는 관련 사건의 조사 원인 분석 및 대책 마련 외의 목적으로는 사용하지 아니한다.

제15조(조사결과의 보고 등) ① 조사관은 사건에 대한 조사를 마친 때에는 다음 각 호의 사항을 기재한 조사결과 보고서를 작성하여 해당 국장에게 보고하여야 한다.

1. 조사배경
2. 조사대상 및 기간
3. 조사경과
4. 위법사실 및 시정조치 등 처리 의견
5. 관계 법령 등 참고 사항
6. 그 밖에 필요한 사항

② 해당 국장은 조사결과에 사실의 오인, 법령의 해석이나 적용의 착오가 있거나 조사 이후 새로운 사실 또는 증거의 발견이 있는 경우 등에는 조사관에게 보완조사를 명할 수 있다. 이 경우 조사관은 최초 결과보고와 조사내용이 달라지는 경우에는 해당 국장에게 수정보고할 수 있다.

제15조의2(조사종결 등) ① 해당 국장은 다음 각 호의 어느 하나의 경우에는 조사를 종결할 수 있다.

1. 조사를 개시하였으나 제5조의2에 따라 조사에 착수하지 않을 수 있는 경우에 해당하는 경우
2. 조사대상자에게 사망, 청산 또는 이에 준하는 사유가 발생함으로써 조사를 하기가 사실상 불가능하다고 인정되는 경우
3. 조사대상자의 행위가 위반행위로 인정되지 않거나 증거가 존재하지 않는 등 법 위반 여부의 판단이 불가능하거나 시정조치 등의 처분이 필요하지 않다고 인정되는 경우
4. 정보주체의 개인정보에 관한 권리 또는 이익 침해 사실이 없는 것으로 인정되는 경우
5. 제1호부터 제4호까지에 준하는 경우

② 해당 국장은 조사대상자에게 영업 재개 등의 조사 개시 사유가 발생한 때에는 종결된 조사의 재개를 명할 수 있다.

제15조의3(사건의 전결) 해당 국장은 보호위원회의 결정과 유사·반복되는 사건으로서 위원장이 전결할 필요가 있다고 인정하는 사건의 경우에는 다음 각 호의 어느 하나에 해당하는 전결을 할 수 있다.

1. 제21조의 경고에 해당한다고 인정되는 사건에 대한 경고
2. 제23조의 주의촉구에 해당한다고 인정되는 사건에 대한 주의촉구

제15조의4(종결 및 전결의 통지) ① 보호위원회는 제15조의2제1항에 따라 조사를 종결하거나 제15조의3

에 따라 전결한 경우에는 종결 또는 전결이 있은 날부터 14일 이내에 조사대상자에게 그 사실을 통지하여야 하며, 신고인(보호위원회가 필요하다고 인정하는 경우에는 이해관계인 등을 포함한다)에게는 그 요지를 통지할 수 있다.

② 제1항에도 불구하고 제15조의2제1항에 따른 조사종결 사건으로서 조사대상자에게 통지가 불가능한 경우에는 조사대상자에게 통지하지 않을 수 있다.

제3절 시정조치안의 작성

제16조(사전통지 등) ① 조사관은 제15조제1항에 따른 조사결과 보고서를 근거로 예정된 제18조제2항 각 호의 시정조치(법 제61조제2항에 따른 개선권고 및 법 제65조에 따른 고발은 제외하며, 이하 이 조 및 제16조의2에서 "처분"이라 한다)에 대하여 다음 각 호의 사항을 기재한 사전통지서를 제15조제1항에 따라 조사결과 보고를 마친 날부터 14일 이내에 처분을 받은 자(이하 이 조 및 제16조의2에서 "당사자"라 한다)에게 통지하고, 14일 이상의 기간을 정하여 의견을 제출할 기회를 주어야 한다.

1. 당사자의 성명(법인인 경우에는 법인의 명칭 및 대표자의 성명), 주소
2. 처분의 원인이 되는 사실과 처분의 내용 및 적용 법령
3. 제2호에 대하여 의견을 제출할 수 있다는 사실과 의견을 제출하지 않는 경우의 처리방법

3의2. 보호위원회가 안건 심의 등을 위해 필요하다고 인정한 때에는 보호위원회에 출석하여 의견을 진술할 수 있다는 사실 및 의견을 진술하고자 할 때에는 미리 그 사실 및 그 의견의 요지를 보호위원회에 알려야 한다는 사실

4. 보호위원회의 명칭과 주소(전자우편주소를 포함한다)
5. 의견제출 기한
6. 증거자료 목록
7. 사무처의 조치의견은 보호위원회를 기속하지 아니한다는 내용
8. 그 밖에 필요한 사항

② 조사관은 과징금 또는 과태료의 부과가 필요하다고 인정되는 사건의 경우에는 당사자의 방어권이 보장될 수 있도록 과징금 또는 과태료 부과기준 관련 내용이 포함된 서면을 포함하여 당사자에게 사전통지서를 통지하거나 관련 내용을 충분히 설명하여야 한다.

③ 조사관은 제1항에 따라 조사대상자에게 사전통지서를 통지한 이후 보완조사 등으로 처분의 원인이 되는 사실과 처분의 내용 및 적용 법령 등이 달라지는 경우(처분을 하지 않거나 처분이 완화되는 경우는 제외한다)에는 조사대상자에게 다시 사전통지서를 통지하여야 한다.

제16조의2(의견제출 등) ① 제16조에 따른 사전통지서를 받은 당사자 또는 그가 지정한 대리인은 서면(전자문서를 포함한다)으로 의견을 제출하거나 말로 의견을 진술할 수 있고, 그 주장을 증명하기 위하여 증거자료를 제출할 수 있다. 당사자가 말로 의견을 진술한 경우에는 조사관은 진술자와 그 의견의 요지를 기록하여 당사자로 하여금 진술내용을 확인하게 한 후 서명 또는 날인하도록 하여야 한다.

② 다음 각 호의 어느 하나에 해당하는 경우에는 경우에는 당사자의 의견이 없는 것으로 본다.

1. 당사자가 제16조에 따른 사전통지서에 기재된 기일까지 의견제출을 하지 않은 경우
2. 당사자가 제1항 후단에 따라 말로 의견을 진술한 경우로서 조사관이 그 의견의 요지를 기록한 문서에 당사자가 서명 또는 날인하지 않은 경우

③ 당사자는 제16조에 따른 사전통지서에 기재된 처분의 내용에 과징금의 부과가 포함되어 있는 경우에는 사전통지서에 기재된 기일까지 재무제표 등 회계자료, 매출액 산정자료 등 매출액 입증자료(이하 "입증자료"라 한다)를 제출하여야 하며, 입증자료를 제출하지 못하는 정당한 사유가 있을 때에는 그 사유를 제출하여야 한다.

④ 보호위원회는 제1항에 따라 당사자가 제출한 의견에 상당한 이유가 있는 경우에는 처분을 하지 않거나 처분의 내용을 변경할 수 있다.

⑤ 당사자는 보호위원회가 안건 심의 등을 위해 필요하다고 인정한 경우로서 보호위원회에 출석하여

의견을 진술하고자 할 때에는 미리 그 사실 및 그 의견의 요지를 보호위원회에 알려야 한다. 이 경우 당사자의 출석 및 의견진술에 관하여는 「개인정보 보호위원회 운영규칙」 제11조제2항 및 제3항에서 정하는 바에 따른다.

제17조(증거자료 열람·복사 등) ① 제16조에 따라 사전통지서를 송달받은 당사자는 사전통지서에 기재된 증거자료를 특정하여 보호위원회에 열람·복사를 신청할 수 있다.

② 조사관은 제1항에 따른 열람·복사 신청이 있는 때에는 다음 각 호의 어느 하나에 해당하는 사유를 제외하고는 이를 허가하여야 한다.

1. 영업비밀 보호
2. 사생활의 비밀 보호
3. 법령에 따른 비공개 자료
4. 기타 공익상 열람·복사를 허가함이 적절하지 아니하다고 판단되는 경우

제18조(시정조치안의 작성) ① 해당 국장은 제15조제1항에 따른 조사결과 보고서를 근거로 제16조의2에 따른 피심인의 의견제출 내용을 포함하여 시정조치안을 작성하여야 한다.

② 시정조치안은 다음 각 호의 사항을 포함하되, 구체적 내용은 위반행위의 정도와 시정조치에 따른 효과 등을 고려하여 결정한다.

1. 법 제64조제1항에 따른 시정조치 명령 및 신용정보법 제45조의4에 따른 시정조치(이하 "시정조치 명령"이라 한다), 법 제64조제3항에 따른 시정권고(이하 이 장에서 "시정권고"라 한다)
2. 법 제64조의2 및 신용정보법 제42조의2에 따른 과징금의 부과
3. 법 제75조 및 신용정보법 제52조에 따른 과태료의 부과
4. 법 제65조에 따른 고발 및 징계권고
5. 법 제66조에 따른 결과의 공표 및 공표명령
6. 법 제61조제2항에 따른 개선권고

제18조의2(재조사 등) 위원장은 다음 각 호의 어느 하나의 경우에는 해당 국장에게 해당 사건에 대한 보완조사 또는 재조사를 명할 수 있다.

1. 조사결과 또는 시정조치안에 사실의 오인, 법령의 해석이나 적용의 착오가 있는 경우
2. 제15조의2제1항에 따른 조사종결이 있은 후 새로운 사실 또는 증거의 발견이 있는 경우

제4절 시정조치안의 심의·의결 및 이행점검

제19조(시정조치안의 심의·의결) ① 해당 국장은 제18조에 따라 작성한 시정조치안을 보호위원회에 심의·의결안건으로 상정하여야 한다. 다만, 위반행위가 경미하거나 유사·반복되는 위반행위에 대한 시정조치 명령 또는 과태료의 부과 등에 해당하여 위원장이 법 제7조의12에 따른 소위원회(이하 "소위원회"라 한다)가 심의·의결할 필요가 있다고 인정하는 사항에 대해서는 소위원회에 상정할 수 있다.

② 보호위원회는 시정조치안을 의결하기 위하여 필요한 경우에는 피심인 및 이해관계인의 의견진술, 관계전문가의 자문 등의 절차를 거칠 수 있다.

③ 그 밖에 보호위원회의 의결에 필요한 사항은 「개인정보 보호위원회 운영규칙」이 정하는 바에 따른다.

제20조(시정조치 명령 등) 보호위원회는 법 위반 또는 침해 상태의 해소를 위해 시정조치를 명하거나 권고할 때에는 상당한 기간을 정하여 해당 위반행위 또는 침해행위에 대한 시정을 명하거나 권고하여야 한다.

제21조(경고) 보호위원회는 다음 각 호의 어느 하나에 해당하여 시정조치의 실익이 없는 경우에는 경고를 의결할 수 있다.

1. 개인정보 침해 정도가 경미한 경우
2. 피심인이 위반행위를 스스로 시정한 경우
3. 과징금 및 과태료를 부과하지 않을 수 있는 경우

제22조(사건종결) 보호위원회는 다음 각 호의 어느 하나의 경우에는 사건종결을 의결할 수 있다.
1. 피심인에게 사망, 청산 또는 이에 준하는 사유가 발생함으로써 시정조치의 이행을 확보하기가 사실상 불가능하다고 인정되는 경우
2. 피심인의 행위가 위반행위로 인정되지 않거나 증거가 존재하지 않는 등 법 위반 여부의 판단이 불가능하거나 시정조치 등의 처분이 필요하지 않다고 인정되는 경우
3. 정보주체의 개인정보에 관한 권리 또는 이익 침해 사실이 없는 것으로 인정되는 경우
4. 제1호부터 제3호까지에 준하는 경우

제23조(주의촉구) 보호위원회는 피심인의 행위가 법에 위반되지 아니하더라도 장래의 법 위반 예방 등 필요한 경우에는 주의촉구를 할 수 있다.

제24조(심의중지) ① 보호위원회는 제8조의3제1항 각 호의 어느 하나에 해당하는 경우로서 심의를 계속할 수 없는 사유가 있는 경우에는 그 사유가 해소될 때까지 심의중지를 의결할 수 있다. 이 경우 제8조의3제1항 각 호 중 "조사"는 "심의"로, "조사대상자"는 "피심인"으로 본다.

② 조사관은 제1항에 따라 심의중지가 의결된 때에는 심의중지 사유가 해소되었는지 여부를 점검 및 관리하여야 한다.

③ 보호위원회는 심의중지가 의결된 날부터 6개월이 경과한 후에도 그 사유가 해소되지 않은 경우에는 제22조에 따른 사건종결을 의결할 수 있다. 이 경우 보호위원회는 의결서에 "피심인에게 영업 재개 등의 심의 재개 사유가 발생한 때에는 심의절차를 재개할 수 있다"는 문구를 명백히 기재하여야 한다.

제24조의2(심의의 분리·병합 및 재개) 위원장은 필요하다고 인정할 때에는 안건 및 심의 절차의 분리·병합 및 그 취소 또는 종결된 심의절차의 재개를 명할 수 있다.

제25조(의결서의 작성) ① 보호위원회는 제19조부터 제23조까지에 따른 의결사항에 대하여 그 의결이 있은 날부터 30일 이내에 다음 각 호의 사항을 기재한 의결서를 작성하여야 한다. 다만, 부득이한 사유로 인하여 작성기간의 연장이 필요한 경우에는 연장되는 기간을 정하여 위원장의 허가를 받아야 한다.
1. 안건번호 및 안건명
2. 피심인
3. 의결연월일
4. 주문
5. 이유
6. 이의제기 방법 및 기간

② 보호위원회는 「개인정보 보호위원회 운영규칙」 제7조에도 불구하고 다음 각 호의 어느 하나에 해당하는 의결사항의 경우에는 제1항 각 호의 내용을 약식으로 기재한 의결서를 작성할 수 있다.
1. 법 제61조제2항에 따른 개선권고를 명하는 사건
2. 제21조에 따른 경고를 명하는 사건
3. 제22조에 따른 사건종결을 의결하는 사건
4. 제23조에 따른 주의촉구를 하는 사건
5. 제19조제1항 단서에 따라 소위원회에서 심의·의결한 사건

③ 제1항 및 제2항에 따라 작성한 의결서에는 해당 심의·의결에 참여한 위원이 서명 또는 날인하여야 한다.

④ 보호위원회는 둘 이상의 안건을 하나의 의결서로 작성할 수 있다. 다만, 피심인이 2인 이상인 경우로서 피심인의 영업비밀, 사생활의 비밀, 그 밖에 정당한 이익을 해칠 우려가 있는 경우에는 그렇지 않다.

제25조의2(의결서의 통지) ① 조사관은 제25조에 따라 작성한 의결서에 참여 위원의 서명 또는 날인을 받은 경우 지체 없이 그 정본(의결서가 생산되지 않은 경우에는 그 의결 취지, 내용을 말한다)을 피심인에게 송달하여야 하며, 신고인(보호위원회가 필요하다고 인정하는 경우에는 이해관계인 등을 포함한다)에게는 그 요지를 통지할 수 있다.

② 제1항에도 불구하고 제22조에 따른 사건종결을 의결하는 사건으로서 피심인에게 송달이 불가능한 경우에는 피심인에게 송달하지 않을 수 있다.

③ 시정조치 명령 및 과징금 부과처분 등의 시정조치는 의결서를 송달받은 날로부터 효력이 발생한다.

제25조의3(의결서의 공개) 의결서는 공개를 원칙으로 한다. 다만, 의결서의 전부 또는 일부가 「개인정보 보호위원회 운영규칙」 제12조제1항 각 호 어느 하나에 해당하는 경우에는 이를 공개하지 않거나 해당 부분에 대해 비식별화 조치 등을 하고 공개할 수 있다.

제26조(공표시기) 법 제66조제1항에 따라 시정조치의 결과를 공표할 때에는 해당 시정조치에 대한 의결서를 발송한 날에 공표한다. 다만, 보호위원회가 필요하다고 인정하는 경우에는 공표시기를 달리 정할 수 있다.

제27조(명령 등 이행 여부의 확인) ① 피심인은 시정조치 명령, 시정권고 또는 공표명령(이하 이 조에서 "시정명령등"이라 한다)의 이행 결과를 보호위원회가 정한 기간 내에 보호위원회에 알려야 한다.

② 피심인은 부득이한 사유로 시정명령등의 이행완료 기한의 연장이 필요한 경우에는 이행완료 기한이 경과하기 전에 연장사유 및 기간을 보호위원회에 알리고 보호위원회와 협의하여야 하며, 보호위원회는 피심인이 시정명령등의 이행 기한 내에 시정명령등을 이행할 수 없다고 인정하는 경우에는 1회에 한하여 그 기간의 연장을 허용할 수 있다.

③ 해당 국장은 피심인이 시정명령등을 이행하였는지 여부를 연 2회(6월, 12월) 확인하여야 한다.

④ 해당 국장은 피심인이 시정명령등을 이행하지 않은 경우에는 이를 보호위원회에 보고하여야 한다.

제27조의2(개선권고 및 징계권고 통보 여부의 확인) ① 피심인은 법 제61조제2항에 따른 개선권고 및 제65조제2항에 따른 징계권고(이하 이 조에서 "개선권고등"이라 한다)의 결과를 보호위원회가 정한 기간 내에 보호위원회에 알려야 한다.

② 피심인은 부득이한 사유로 개선권고등의 결과 통보 기한의 연장이 필요한 경우에는 결과 통보 기한이 경과하기 전에 연장사유 및 기간을 보호위원회에 알리고 보호위원회와 협의하여야 하며, 보호위원회는 피심인이 개선권고등의 결과 통보 기한 내에 개선권고등 결과를 통보할 수 없다고 인정하는 경우에는 1회에 한하여 그 기간의 연장을 허용할 수 있다.

③ 해당 국장은 피심인이 개선권고등의 결과를 통보하였는지 여부를 연 2회(6월, 12월) 확인하여야 한다.

④ 해당 국장은 피심인이 개선권고등의 결과를 통보하지 않은 경우에는 이를 보호위원회에 보고하여야 한다.

제5절 이의제기 등

제28조(과징금 부과처분 등에 대한 이의제기) ① 피심인은 보호위원회의 시정조치 명령 및 과징금 부과처분 등의 행정처분(과태료 부과처분은 제외한다)에 불복이 있는 경우에는 「행정심판법」 제27조 및 「행정소송법」 제20조에 따라 그 처분이 있음을 알게 된 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

② 제1항에 따른 행정심판 및 행정소송에 관하여는 「행정심판법」 및 「행정소송법」을 따른다.

제29조(과태료 부과처분에 대한 이의제기) ① 피심인은 보호위원회의 과태료 부과처분에 불복이 있는 경우에는 「질서위반행위규제법」 제20조에 따라 과태료 부과 통지를 받은 날부터 60일 이내에 보호위원회에 서면으로 이의제기를 할 수 있다.

② 제1항에 따른 이의제기가 있는 경우에는 보호위원회의 과태료 부과처분은 그 효력을 상실하고, 관할 법원(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판절차에 따라 결정한다. 이 경우 당사자는 관할 법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납부 의무를 부담한다.

③ 보호위원회는 제1항에 따른 이의제기를 받은 경우에는 「질서위반행위규제법」 제21조에 따라 이의제기를 받은 날부터 14일 이내에 이에 대한 의견 및 증빙서류를 첨부하여 관할 법원에 통보하여야 한다.

④ 제1항부터 제3항까지에서 규정하지 않은 과태료 부과처분에 대한 이의제기 및 재판 등의 절차에 관하여는 「질서위반행위규제법」을 따른다.

제3장 사전 실태점검

제30조(사전 실태점검의 착수 등) ① 해당 국장은 법 제63조제1항 각 호에 해당하지 아니하는 경우로서 개인정보 침해사고 발생의 위험성이 높고 개인정보 보호의 취약점을 사전에 점검할 필요성이 인정되는 경우에는 이를 담당할 조사관을 지정하여 사전 실태점검에 착수할 수 있다. 이 경우 조사관은 사건의 개요, 사전 실태점검 방법 및 일정 등을 포함한 사전 실태점검 착수 보고서를 작성하여 해당 국장에게 보고하여야 한다.

② 제1항에도 불구하고 해당 국장은 사전 실태점검의 착수에 필요한 사실관계의 확인 등 사전검토를 할 수 있다.

제30조의2(합동 사전 실태점검) 보호위원회는 법 제63조의2제6항에 따라 관계 중앙행정기관의 장과 합동으로 개인정보 보호실태를 점검할 수 있다.

제30조의3(시정권고안의 작성) ① 해당 국장은 사전 실태점검 결과 보고서를 근거로 제30조의9에 따라 준용되는 제16조의2에 따른 피심인의 의견제출 내용을 포함하여 시정권고안을 작성하여야 한다.

② 시정권고안은 법 제63조의2제2항에 따른 시정권고를 포함하되, 구체적 내용은 위반행위의 정도와 시정권고에 따른 효과 등을 고려하여 결정한다.

제30조의4(시정권고) 보호위원회는 법 제63조의2에 따른 사전 실태점검을 실시하여 법을 위반하는 사항을 발견한 경우 피심인에 대하여 시정방안(피심인이 해당 권고를 수락하는 경우의 해당 권고의 이행기간을 포함한다)을 정하여 이에 따를 것을 권고할 수 있다.

제30조의5(의결서의 작성) 보호위원회는 제30조의4에 따른 시정권고(이하 이 장에서 "시정권고"라 한다)에 대하여 그 의결이 있은 날부터 30일 이내에 다음 각 호의 사항을 기재한 의결서를 작성하여야 한다. 다만, 부득이한 사유로 인하여 작성기간의 연장이 필요한 경우에는 연장되는 기간을 정하여 위원장의 허가를 받아야 한다.

1. 안건번호 및 안건명
2. 피심인
3. 의결연월일
4. 주문(피심인이 해당 권고를 통보받은 날부터 10일 이내에 해당 권고를 수락하는지 여부에 관하여 보호위원회에 통지해야 한다는 사실을 포함한다)
5. 이유
6. 지정된 기일까지 피심인의 통지가 없는 경우에는 해당 권고를 수락하지 않은 것으로 본다는 사실
7. 피심인이 해당 권고를 수락하지 않거나 이행하지 않은 경우 보호위원회는 법 제63조제2항에 따른

검사를 할 수 있다는 사실

8. 이의제기 방법 및 기간

제30조의6(시정권고의 수락 여부 통지) ① 시정권고를 받은 피심인은 법 제63조의2제3항에 따라 이를 통보받은 날부터 10일 이내에 해당 권고를 수락하는지 여부에 관하여 보호위원회에 통지해야 한다.

② 전항에 따라 지정된 기일까지 피심인의 통지가 없는 경우에는 해당 권고를 수락하지 않은 것으로 본다.

제30조의7(시정권고 이행 여부의 확인 등) 피심인은 법 제63조의2제3항에 따라 시정권고의 이행 결과를 보호위원회가 정한 기간 내에 보호위원회에 알려야 한다.

제30조의8(시정권고 미이행 등에 따른 검사) 보호위원회는 시정권고를 받은 피심인이 해당 권고를 수락하지 아니하거나 이행하지 아니한 경우에는 법 제63조제2항에 따른 검사를 할 수 있다. 이 경우 조사 및 처분에 관하여는 제2장에서 정하는 바에 따른다.

제30조의9(조사 규정의 준용) 사전 실태점검 및 시정권고에 관하여는 제5조제3항, 제6조의2부터 제11조의2까지, 제12조의2부터 제15조의2까지, 제15조의4부터 제17조까지, 제18조의2, 제19조, 제25조제3항 및 제27조제2항부터 제4항까지를 준용한다. 이 경우 "조사"는 "사전 실태점검"으로, "처분", "시정조치", "시정명령등"은 각각 "시정권고"로 본다.

제4장 업무의 위탁 등

제31조(업무의 위탁 등) ① 보호위원회는 영 제62조제3항에 따라 다음 각 호의 어느 하나에 해당하는 사항과 관련된 접수 및 조사를 전문기관에 위탁할 수 있다. 다만, 제2항 각 호의 어느 하나에 해당하는 사건은 그렇지 않다.

1. 법 제62조에 따라 개인정보 침해신고센터에 접수된 신고(다른 기관에 접수된 신고로서 개인정보 침해신고센터에서 처리할 필요성이 인정되는 신고를 포함한다. 이하 같다)
2. 법 제34조제3항 전단에 따른 신고에 대한 기술지원

② 제1항 단서에 해당하는 사건은 다음 각 호와 같다.

1. 위반행위의 정도가 상당한 사건
2. 불특정 다수의 정보주체에게 상당한 피해가 발생하였거나 발생할 가능성이 상당한 사건
3. 특정 분야에 속한 다수 개인정보처리자들의 동일한 위반행위 관련 사건
4. 조사착수 시 조사기간이 6개월을 초과하여 정하여지는 등 조사내용이 복잡한 사건
5. 사회에 미치는 영향 등으로 대응이 시급한 사건
6. 공동조사 또는 국제협력이 필요한 사건
7. 제1호부터 제6호까지에 준하는 사건

제31조의2(조사의 착수 등) ① 전문기관은 제31조에 따라 신고를 접수한 경우로서 조사의 필요성이 인정되는 경우에는 조사에 착수하여야 한다. 이 경우 전문기관은 제6조에 따른 조사착수 보고서를 작성하여야 한다.

② 제1항에도 불구하고 전문기관은 조사착수에 필요한 사실관계의 확인 등 사전검토를 할 수 있다.

③ 전문기관은 신고를 접수한 날부터 14일 이내에 조사착수 여부의 결정을 마쳐야 한다. 다만, 사실관계가 복잡한 사건의 경우에는 14일 이내로 기간을 연장할 수 있다.

제31조의3(조사기간) ① 전문기관이 조사를 하는 경우 사건의 조사개시일은 제31조의2제1항에 따른 조사착수 보고일로 한다.

② 전문기관은 조사개시일로부터 6개월 이내에 보호위원회에 제31조의4에 따른 조사결과 자료 송부를 마쳐야 한다. 다만, 부득이한 사유로 조사기간의 연장이 필요한 경우에는 조사기간이 경과하기 전에 연장기간을 정하여 조사기간을 연장할 수 있다.

제31조의4(조사결과 자료의 송부 등) ① 전문기관은 사건에 대한 조사를 마친 때에는 보호위원회에 조사결과 자료를 송부하여야 한다.

② 보호위원회는 전문기관이 작성한 조사결과 자료를 검토하여 조사결과에 사실의 오인, 법령의 해석이나 적용의 착오가 있거나 조사 이후 새로운 사실 또는 증거의 발견이 있는 경우 등에는 전문기관에 보완조사를 요구하거나 직접 보완조사를 할 수 있다.

제31조의5(조사종결 등) ① 전문기관은 제15조의2제1항 각 호의 어느 하나에 해당한다고 인정되는 사건에 대하여는 조사를 종결할 수 있다.

② 전문기관은 조사대상자에게 영업 재개 등의 조사 개시 사유가 발생한 때에는 종결된 조사를 재개할 수 있다.

제31조의6(사건의 전결) 전문기관은 보호위원회의 결정과 유사·반복되는 사건으로서 보호위원회가 전결할 필요가 있다고 인정하는 사건의 경우에는 다음 각 호의 어느 하나에 해당하는 전결을 할 수 있다.

1. 제21조의 경고에 해당한다고 인정되는 사건에 대한 경고
2. 제23조의 주의촉구에 해당한다고 인정되는 사건에 대한 주의촉구

제31조의7(결과 보고) 전문기관은 법 제68조제2항에 따라 그 결과를 정기적으로 보호위원회에 통보하여야 한다.

제31조의8(조사 규정의 준용) 전문기관의 신고의 접수 및 조사에 관하여는 제4조제1항 및 제2항, 제5조제3항, 제5조의2, 제6조의2, 제7조의2부터 제11조의2까지, 제12조의2부터 제14조까지 및 제15조의4를 준용한다. 이 경우 "보호위원회", "해당 국장" 또는 "조사관"은 각각 "전문기관"으로 본다.

제5장 보칙

제32조(세부사항 시행) ① 위원장은 이 규정의 세부사항을 시행하기 위하여 필요한 경우 각종 지침이나 서식 등을 정할 수 있다.

② 전문기관은 관계 법령, 행정규칙 및 이 규정에서 규정한 사항 외에 이 규정에 따른 전문기관의 조사 및 처리에 필요한 세부사항을 정할 수 있다.

제33조(재검토 기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 규정에 대하여 2023년 9월 15일을 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-9호, 2023. 10. 16.>

제1조(시행일) 이 규정은 발령한 날부터 시행한다.

제2조(계속 사건에 관한 적용례) 이 규정은 이 규정 시행 당시 조사가 계속 중인 사건에 대해서도 적용한다.

제3조(기간에 관한 적용례) ① 제5조제2항 및 제31조의2제3항의 개정규정은 이 규정 시행 이후 접수되는 신고부터 적용한다.

② 제16조제1항의 개정규정은 이 규정 시행 이후 조사결과 보고를 마친 사건부터 적용한다.

제4조(업무의 위탁에 관한 적용례) 제31조의 개정규정은 이 규정 시행 이후 접수되는 신고부터 적용한다.

9 기타사항

1 아동의 개인정보 (법 제22조의2)

1. 개정 개요

□ 14세 미만 아동에 대한 특별한 보호를 위해 종전의 특례규정과 일반규정에 분산되어 있던 규정을 정비하여 체계화하였다.

□ 아동의 개인정보 처리 시 법정대리인의 동의의무 및 법정대리인 동의 확인의무, 알기 쉬운 언어 사용 등의 의무를 모든 개인정보처리자로 확대하였다.

2. 법령

법률	**제5조(국가 등의 책무)** ① ~ ② (생 략) ③ 국가와 지방자치단체는 만 14세 미만 아동이 개인정보 처리가 미치는 영향과 정보주체의 권리 등을 명확하게 알 수 있도록 만 14세 미만 아동의 개인정보 보호에 필요한 시책을 마련하여야 한다. **제22조의2(아동의 개인정보 보호)** ① 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 하며, 법정대리인이 동의하였는지를 확인하여야 한다. ② 제1항에도 불구하고 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보로서 대통령령으로 정하는 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다. ③ 개인정보처리자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 할 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다. ④ 제1항부터 제3항까지에서 규정한 사항 외에 동의 및 동의 확인 방법 등에 필요한 사항은 대통령령으로 정한다.
시행령	**제17조의2(아동의 개인정보 보호)** ① 개인정보처리자는 법 제22조의2제1항에 따라 법정대리인이 동의했는지를 확인하는 경우에는 다음 각 호의 어느 하나에 해당하는 방법으로 해야 한다. 1. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 개인정보처리자가 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법 2. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법 3. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통하여 본인 여부를 확인하는 방법 4. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나 우편 또는 팩스를 통하여 전달하고, 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법 5. 동의 내용이 적힌 전자우편을 발송하고 법정대리인으로부터 동의의 의사표시가 적힌 전자우

	편을 전송받는 방법 6. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 받거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 받는 방법 7. 그 밖에 제1호부터 제6호까지의 규정에 준하는 방법으로서 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법 ② 법 제22조의2제2항에서 "대통령령으로 정하는 정보"란 법정대리인의 성명 및 연락처에 관한 정보를 말한다. ③ 개인정보처리자는 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우에는 인터넷주소 또는 사업장 전화번호 등 동의 내용을 확인할 수 있는 방법을 법정대리인에게 안내할 수 있다.

3. 개정내용 해설

□ 14세 미만 아동에 대한 특별한 보호를 위해 종전의 정보통신서비스 특례규정과 일반규정에 분산되어 있던 규정을 정비하여 체계화하였고,

○ 법 제5조제3항 신설을 통해 국가 및 지방자치단체로 하여금 아동의 개인정보 보호에 관한 종합적인 시책을 마련하도록 하였다.

□ 그동안 정보통신서비스 제공자에게만 적용되던 법정대리인 동의의 확인 방법, 14세 미만 아동에 대한 개인정보 처리에 관한 고지 방법 등의 특례규정이 모든 개인정보처리자로 확대되었다.

○ 따라서 개인정보처리자는 법정대리인의 동의를 받는 경우 동의가 형식적으로 이루어지는 사례가 발생하지 않도록 법정대리인이 실제로 동의 하였는지 확인해야 하며,

○ 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 할 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용해야 한다.

4. 개인정보처리자 유의사항

□ 기존 온라인 사업자(정보통신서비스 제공자)의 경우 기존 아동에 대한 개인정보 보호 처리에 크게 달라지는 점은 없으나,

○ 공공기관, 오프라인 사업자 등 기존에 일반규정을 적용받고 있던 개인정보처리자는 2023년 9월 15일부터 14세 미만 아동의 개인정보 수집·이용 동의 시에 법정대리인 동의 확인, 아동에 대한 고지 등에 유의해야 한다.

5. 제재 규정

위반행위	제재 내용
법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 처리한 경우 (제22조의2제1항 위반, 제26조제8항에 따라 준용되는 경우를 포함)	과징금 부과 (제64조의2제1항제2호)
법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 처리한 자 (제22조의2제1항 위반, 제26조제8항에 따라 준용되는 경우를 포함)	5년 이하의 징역 또는 5천만원 이하의 벌금(제71조제3호)

※ 법정대리인이 동의하였는지를 확인해야 하는 의무에 대한 형벌 규정은 삭제

2 민감정보 처리 제한 (법 제23조)

1. 개정 개요

□ 서비스 제공 과정에서 공개되는 정보에 정보주체 스스로가 입력한 민감정보가 포함되어 사생활 침해 위험이 있다고 판단하는 때에는,

○ 서비스 제공 전에 '민감정보가 공개될 수 있다는 사실'과 원하지 않을 경우 '비공개로 선택하는 방법'을 정보주체가 알아보기 쉽게 알리도록 하였다.

2. 법령

법률	**제23조(민감정보의 처리 제한)** ①개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 ② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다. ③ 개인정보처리자는 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알려야 한다. **제30조(개인정보 처리방침의 수립 및 공개)** ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. 1 ~ 3의2. (생 략) 3의3. 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)

3. 개정내용 해설

□ 개인정보처리자는 재화 또는 서비스를 제공하는 과정에서 정보주체인 국민의 민감정보가 의도치 않게 공개되어 사생활이 침해되지 않도록, 재화 또는 서비스의 제공 전에 경고창 등을 통해 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알려야 한다.

○ 다만, 공개 게시판, 소셜네트워크서비스(SNS) 등 서비스 자체가 공개를 기본으로 하여 상호 의사소통을 목적으로 하고 있어 정보주체가 공개 게시판 등에 스스로 입력하는 정보가 공개된다는 사실을 이미 알고 있다고 볼 수 있는 경우에는 공개 가능성 등을 알리지 않을 수 있다.

□ 개인정보처리자는 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 경고창 등을 활용하여 정보주체가 알아보기 쉽게 알리고, 개인정보처리방침을 통해 공개 가능성 및 비공개를 선택하는 방법을 공개해야 한다.(법 제30조제1항제3호의3)

사례 온라인 지도앱 서비스에서 민감정보가 공개된 사례

· 지도앱 서비스 이용자가 스스로 정보를 입력하여 저장한 폴더가 기본설정이 공개로 되어 있는 사실을 모른 채 성생활, 건강 등 민감한 정보를 입력하여 인터넷에 공개된 사례('21.1월)

4. 개인정보처리자 유의사항

○ 정보주체가 해당 서비스를 이용하는 과정에서 자신이 스스로 입력한 정보에 대한 공개 기능이 있는 경우에는 비공개를 기본으로 설정하여 운영하고, 정보주체가 공개를 원할 경우 스스로 공개 여부를 결정할 수 있도록 할 필요가 있다.

5. 제재 규정

위반행위	제재 내용
민감정보의 공개 가능성 및 비공개를 선택하는 방법을 알리지 아니한 자 (제23조제3항 위반, 제26조제8항에 따라 준용되는 경우를 포함)	3천만원 이하의 과태료 (제75조제2항제6호)

3 업무위탁 처리 제한 (법 제26조)

1. 개정 개요

□ 개인정보 침해사고 발생시 위탁자가 재위탁된 사실을 알 수 없었다는 이유로 수탁자에게 책임을 전가하여 정보주체의 피해구제가 곤란하다는 우려를 반영하여,

○ 정보주체와 위탁자, 수탁자와의 관계에서 정보주체에 대한 실질적인 책임을 위탁자가 부담하고, 수탁자도 법 위반에 대하여 책임이 있는 범위 내에서 책임을 질 수 있도록 개정하였다.

2. 법령

법률	**제26조(업무위탁에 따른 개인정보의 처리 제한)** ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항 ② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(개인정보 처리 업무를 위탁받아 처리하는 자로부터 위탁받은 업무를 다시 위탁받은 제3자를 포함하며, 이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다. ③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다. ④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. ⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다. ⑥ 수탁자는 위탁받은 개인정보의 처리 업무를 제3자에게 다시 위탁하려는 경우에는 위탁자의 동의를 받아야 한다. ⑦ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다. ⑧ 수탁자에 관하여는 제15조부터 제18조까지, 제21조, 제22조, 제22조의2, 제23조, 제24조, 제24조의2, 제25조, 제25조의2, 제27조, 제28조, 제28조의2부터 제28조의5까지, 제28조의7부터 제28조의11까지, 제29조, 제30조, 제30조의2, 제31조, 제33조, 제34조, 제34조의2, 제35조, 제35조의2, 제36조, 제37조, 제37조의2, 제38조, 제59조, 제63조, 제63조의2 및 제64조의2를 준용한다. 이 경우 "개인정보처리자"는 "수탁자"로 본다.

시행령	**제28조(개인정보의 처리 업무 위탁 시 조치)** ① (생 략) ② 법 제26조제2항에서 "대통령령으로 정하는 방법"이란 개인정보 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 위탁자의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하는 방법을 말한다. ③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하여야 한다. 1. 위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법 2. 관보(위탁자가 공공기관인 경우만 해당한다)나 위탁자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는「신문 등의 진흥에 관한 법률」제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법 3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법 4. 재화나 서비스를 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

3. 개정내용 해설

□ 개인정보처리자(위탁자)로부터 개인정보의 처리 업무를 위탁받은 수탁자의 범위에 다시 위탁받은 제3자도 포함하도록 규정(법 제26조제2항)하였다.

○ 위탁자는 정보주체가 언제든지 쉽게 확인할 수 있도록 위탁하는 업무의 내용과 수탁자를 포함하여 홈페이지 등에 공개해야 하며, 이 때 다시 위탁받은 제3자에 대하여는 확인할 수 있는 경로 등을 안내하는 방법으로 공개할 수 있다.

※ (예시) 개인정보처리자(위탁자)가 기존의 수탁자를 개인정보처리방침에 공개하고 있는 경우, 수탁자의 개인정보처리방침 링크 추가를 통해 재수탁자의 위탁업무 내용 등을 알릴 수 있음

□ 개인정보처리자(위탁자)로부터 개인정보의 처리 업무를 위탁받은 수탁자가 제3자에게 다시 위탁하려는 경우에는 위탁자의 동의를 받도록 하였다.

○ 재위탁이 반복되는 경우 개인정보 관리가 취약해질 수 있어 다시 위탁하는 것을 제한하되 다시 위탁이 불가피한 경우에는 위탁자의 동의를 받아 진행될 수 있도록 하였다.

○ 위탁자의 동의는 그 형식을 제한하고 있지 않으므로 개인정보 처리 업무의 성격, 위탁계약의 특성 등에 맞추어 다양한 방식으로 받을 수 있다.

4. 개인정보처리자 유의사항

□ 종전에는 수탁자가 법 위반행위에 대한 책임이 있더라도 과징금·과태료·형벌 적용 규정이 없었으나, 법 개정으로 수탁자의 경우에도 법 위반에 대한 책임 있는 범위에서 과징금·과태료·형벌 등을 적용할 수 있도록 개정하였다.

※ 법 제26조제8항 수탁자 준용 규정에 수탁자에게 적용될 수 있는 규정을 추가하였고, 과징금(제64조의2)·형벌(제71~73조)·과태료(제75조) 규정에 개별 위반행위에 따른 제재규정을 추가함

5. 제재 규정

위반행위	제재 내용
위탁자가 관리·감독 또는 교육을 소홀히 하여 수탁자가 이 법의 규정을 위반한 경우(제26조제4항 위반)	과징금 (제64조의2제1항제5호)
개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자(제26조제5항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금(제71조제2호)
정보주체에게 알려야 할 사항을 알리지 아니한 자(제26조제3항 위반)	3천만원 이하의 과태료 (제75조제2항제12호)
위탁자의 동의를 받지 아니하고 제3자에게 다시 위탁한 자(제26조제6항 위반)	2천만원 이하의 과태료 (제75조제3항제1호)
업무 위탁 시 같은 항 각 호의 내용이 포함된 문서로 하지 아니한 자(제26조제1항 위반)	1천만원 이하의 과태료 (제75조제4항제4호)
위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자(제26조제2항 위반)	1천만원 이하의 과태료 (제75조제4항제5호)

4 국내대리인의 지정(법 제31조의2)

1. 개정 개요

□ 정보주체인 국민의 개인정보 자기결정권의 실질적 행사 및 침해사고 발생 시 신속한 조사·협조를 위해 제도가 도입('19.3.)되었으며,

○ 일정 규모 이상 글로벌 사업자에게 개인정보 보호책임자 업무 등을 대리할 국내대리인 지정 의무(매출액, 보유 개인정보 규모 고려)를 부여하였다.

□ 이번 법 개정을 통해 정보통신서비스 제공자에게만 부과되었던 국내대리인 지정 의무를 개인정보처리자 일반으로 확대하였고,

○ 국내대리인을 지정하여야 하는 대상 기준을 글로벌 사업자의 전체 매출액으로 명확하게 규정하고, 보호위원회의 심의·의결로 법 제63조제1항에 따라 관계 물품·서류 등 제출을 요구받은 자에 대하여 국내대리인 지정 의무를 부여할 수 있도록 시행령 제32조의2를 개정하였다.

2. 법령

법률	**제31조의2(국내대리인의 지정)** ① 국내에 주소 또는 영업소가 없는 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 자는 다음 각 호의 사항을 대리하는 자(이하 "국내대리인"이라 한다)를 지정하여야 한다. 이 경우 국내대리인의 지정은 문서로 하여야 한다. 1. 제31조제3항에 따른 개인정보 보호책임자의 업무 2. 제34조제1항 및 제3항에 따른 개인정보 유출 등의 통지 및 신고 3. 제63조제1항에 따른 물품·서류 등 자료의 제출 ② 국내대리인은 국내에 주소 또는 영업소가 있어야 한다. ③ 개인정보처리자는 제1항에 따라 국내대리인을 지정하는 경우에는 다음 각 호의 사항을 개인정보 처리방침에 포함하여야 한다. 1. 국내대리인의 성명(법인의 경우에는 그 명칭 및 대표자의 성명을 말한다) 2. 국내대리인의 주소(법인의 경우에는 영업소의 소재지를 말한다), 전화번호 및 전자우편 주소 ④ 국내대리인이 제1항 각 호와 관련하여 이 법을 위반한 경우에는 개인정보처리자가 그 행위를 한 것으로 본다.
시행령	**제32조의2(국내대리인 지정 대상자의 범위)** ① 법 제31조의2제1항 각 호 외의 부분 전단에서 "대통령령으로 정하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. 1. 전년도(법인인 경우에는 전 사업연도를 말한다) 전체 매출액이 1조원 이상인 자

	2. 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 국내 정보주체의 수가 일일평균 100만명 이상인 자 3. 법 제63조제1항에 따라 관계 물품·서류 등 자료의 제출을 요구받은 자로서 국내대리인을 지정할 필요가 있다고 보호위원회가 심의·의결한 자 ② 제1항제1호에 따른 전체 매출액은 전년도 평균환율을 적용하여 원화로 환산한 금액을 기준으로 한다.

3. 개정내용 해설

□ 국내에 주소나 영업소가 없는 정보통신서비스 제공자에게만 부과되었던 국내대리인 지정 의무를 개인정보처리자로 확대하였다.

□ 국내대리인 지정이 필요한 사업자의 매출액 및 보유 개인정보 규모 관련 기준을 명확히 하고, 보호위원회 심의·의결로 국내대리인 지정이 필요한 사업자를 선정할 수 있도록 하였다.

○ 매출액 규모 판단 시 국내에서 발생한 매출액으로 한정하지 않으며, 해당 개인정보처리자의 전체 매출액을 기준으로 하며, 저장·관리하고 있는 개인정보 판단은 전년도 10월 1일부터 12월 31일까지 매일 저장·관리되고 있는 개인정보의 정보주체 수의 총합을 92(일)로 나눈 수가 100만명 이상인 경우를 의미한다.

○ 보호위원회의 심의·의결의 경우에는 법 위반 혐의로 자료 제출을 요구받는 등 조사 대상 사업자로서 개인정보보호위원회가 국내대리인 지정이 필요하다고 심의·의결한 개인정보처리자가 대상이 된다.

4. 개인정보처리자 유의사항

□ 국내에 별개의 법인을 설립했다고 하더라도 해당 법인이 서비스를 제공하지 않는다면 '국내에 주소 또는 영업소'가 없는 경우에 해당한다.

※ 입법취지인 우리 국민의 개인정보 고충처리, 개인정보 침해신고 시 규제 집행 가능성 등을 고려하여 영업소인지 여부를 판단

5. 제재 규정

위반행위	제재 내용
국내대리인 지정 의무가 있는 글로벌 사업자가 국내대리인을 지정하지 않은 경우(제31조의2제1항 위반)	2천만원 이하 과태료 (제75조제3항제2호)

6. 질의 응답

□ 글로벌 사업자 국내대리인의 역할은 무엇인지?

⇨ 글로벌 사업자의 국내대리인은 ①개인정보 처리와 관련한 불만 처리 및 피해 구제 등 법 제31조에 따른 개인정보 보호책임자의 업무, ②법 제39조의4에 따른 개인정보의 분실·도난·유출 사실 통지·신고 및 ③법 제63조제1항에 따른 법 위반 등과 관련한 물품·서류 등의 제출 업무를 수행함

□ 국내대리인의 자격요건은 무엇인지?

⇨ 국내대리인은 국내에 주소 또는 영업소가 있는 자연인 또는 법인으로서 국적이 한국일 것을 요하지 않지만, 국내 정보주체의 고충을 처리하고 규제기관에 자료를 제출할 수 있어야 하므로 한국어로 원활한 의사소통이 가능해야 함

□ 국내대리인의 지정 절차는 어떻게 되는지?

⇨ 글로벌 사업자는 국내대리인 지정을 문서로 하여야 하며, 국내대리인의 성명, 주소, 전화번호 및 전자우편 주소를 개인정보 처리방침에 포함하여야 하고, 국내대리인이 변경된 경우 지체없이 개인정보 처리방침을 수정하여야 함

5 개인정보파일 등록 · 공개(법 제32조)

1. 개정 개요

□ 공공기관의 개인정보 보호를 강화하기 위해 '공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일'을 예외 없이 등록·공개 대상에서 제외했던 규정을 삭제하여 등록 및 공개 대상에 포함하고,

○ 대신 일회적으로 운영되는 파일 등 지속적으로 관리할 필요성이 낮다고 인정되는 개인정보파일은 대상에서 제외하는 것으로 개선하였다.

□ 시행령 제33조에서는 지속적으로 관리할 필요성이 낮다고 인정되는 개인정보파일의 범위를 보다 구체화하였다.

* [1.]단순 업무 수행을 위해 운영되며 지속적 관리 필요성이 낮은 파일, [2.]공공의 안전과 안녕을 위해 긴급히 필요한 일시적 파일 [3.]일회적 업무 처리만을 위해 수집되어 저장·기록되지 않는 파일 등

2. 법령

법률	**제32조(개인정보파일의 등록 및 공개)** ① (생략) ② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다. 4. 일회적으로 운영되는 파일 등 지속적으로 관리할 필요성이 낮다고 인정되어 대통령령으로 정하는 개인정보파일 ④ 보호위원회는 정보주체의 권리 보장 등을 위하여 필요한 경우 제1항에 따른 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개할 수 있다.
시행령	**제33조(개인정보파일의 등록사항 등)** ① (생략) ② 법 제32조제2항제4호에서 "대통령령으로 정하는 개인정보파일"이란 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. 1. 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일 2. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일 3. 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일 **제34조(개인정보파일의 등록 및 공개 등)** ①개인정보파일(법 제32조제2항 및 이 영 제33조제2항에 따른 개인정보파일은 제외한다. 이하 이 조에서 같다)을 운용하는 공공기관의 장은 그 운용을 시작한 날부터 60일 이내에 보호위원회가 정하여 고시하는 바에 따라 보호위원회에 법 제32조제1항 및 이 영 제33조제1항에 따른 등록사항(이하 "등록사항"이라 한다)의 등록을 신청하여야 한다. 등록 후 등록한 사항이 변경된 경우에도 또한 같다. ② 보호위원회는 법 제32조제4항에 따라 개인정보파일의 등록 현황을 공개하는 경우 이를 보호위원회가 구축하는 인터넷 사이트에 게재해야 한다.

3. 개정내용 해설

□ 법 제32조제2항제4호 개정에 따라 ‘일회적으로 운영되는 파일 등 지속적으로 관리할 필요성이 낮다고 인정’되어 등록 및 공개의 적용이 제외되는 개인정보파일은 다음과 같다.

○ 첫째, 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일은 대상에서 제외된다.

※ 예) 공공요금 정산, 회의참석자 수당지급 등을 위한 개인정보파일

○ 둘째, 공중위생 등 공공의 안전·안녕을 위해 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일도 대상에서 제외된다.

※ 예) 코로나19 확진환자 관리 명단

○ 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 수집된 개인정보 파일은 대상에서 제외된다.

※ 예) 공공기관이 개최하는 일회성 행사에 등록하는 참가자 명단

□ 다만, 그동안 공공기관이 처리하는 개인정보파일 중에서 대상에서 제외되어왔던 인사기록파일, 비상연락망 등 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일이 새롭게 등록대상이 되며,

○ 법 제58조제1항제1호 삭제에 따라 그동안 등록이 제외되던 「통계법」에 따라 수집되는 개인정보파일도 새롭게 등록 대상이 된다.

○ 다만, 내부적 업무처리만을 위하여 사용되거나 통계법에 따라 수집되는 개인정보파일이라 하더라도, 일회적으로 운영되는 등 지속적으로 관리할 필요성이 낮다고 인정되는 경우 등록·공개 의무 대상에서 제외될 수 있다.

4. 개인정보처리자 유의사항

□ 법 제58조제1항제1호* 적용의 일부 제외 규정이 삭제됨에 따라 2023년 9월 15일 당시 「통계법」에 따라 수집된 개인정보가 포함된 개인정보파일을 운영하고 있는 공공기관은 60일 이내 해당 개인정보파일을 보호위원회에 등록해야 한다.

* 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보

5. 제재 규정

□ 해당사항 없음

6. 질의 응답

□ 내부 직원의 전화번호부, 비상연락망 등 내부 업무처리만을 위한 개인정보파일도 등록해야 하는지?

⇨ 개인정보 보호법이 개정(2023.3.14. 공포)되면서 등록·공개 미적용 대상에서 '내부적 업무처리만을 위하여 사용되는 개인정보파일'이 삭제되었음
따라서 그동안 '내부적 업무처리만을 위하여 사용'된다는 이유로 등록하지 않았던 개인정보파일을 등록·관리하여야 함(2023.9.15.시행)

□ 통계법에 따라 수집되는 개인정보파일도 등록해야 하는지?

⇨ 개인정보 보호법이 개정(2023.3.14. 공포)되면서 보호법의 미적용 대상에서 '공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보'가 삭제되었음
따라서 그동안 '「통계법」에 따라 수집'된다는 이유로 등록하지 않았던 개인정보파일을 등록·관리하여야 함(2023.9.15.시행)

□ 위원회 및 자문회의 참석 수당 지급을 위한 개인정보파일도 등록해야 하는지?

⇨ 위원회 및 회의 참석 수당 지급은 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일에 해당되므로 개인정보파일 등록 대상이 아님

□ 개인정보파일 등록·공개 의무대상에 해당하지 않는 경우 개인정보 처리방침 공개 및 개인정보 영향평가 수행 의무도 면제되는지?

⇨ **(개인정보 처리방침)** 공공기관은 보호법 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정해야 함.(보호법 제30조제1항) 따라서 등록대상에 해당하지 않는 개인정보파일은 처리방침을 통해 공개하지 않아도 되지만, 보호법 개정(2023.3.14. 공포)에 따라 그동안 '내부적 업무처리만을 위하여 사용'되거나, '「통계법」에 따라 수집'되는 등의 이유로 등록하지 않았던 개인정보파일을 신규 등록하고, 개인정보 처리방침 또한 개정하여 해당 내용을 반영하여야 함(2023.9.15.시행)

⇨ **(개인정보 영향평가)** 공공기관의 장은 대통령령으로 정하는 기준*에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선사항 도출을 위해 개인정보 영향평가를 수행해야 하며, 개인정보파일 등록대상에 해당하지 않는다고 하여 개인정보 영향평가 수행 의무가 면제되는 것은 아님. 또한 영향평가를 수행한 개인정보파일을 개인정보위에 등록할 때에는 영향평가 결과를 함께 첨부하여야 함(보호법 제33조제4항)

* ①정보주체 100만명 이상의 개인정보, ②50만명 이상의 연계정보, ③5만명 이상의 민감·고유식별정보의 처리가 수반되는 개인정보파일 등(보호법 제33조 및 영 제35조)

□ 공공기관 내부업무 처리 목적 파일이 등재 대상이 되면서, 예를 들어 내부업무 목적 ERP가 대표적으로 해당하는데, ERP는 인사, 재무 등 다양한 분야가 있음. 원래 개인정보 파일 취지가 업무 단위로 등록하게 되어있는데 이에 대한 표준목록이 개인정보보호위원회에서 나오는지? 내부업무 목적에 따라 등록할 파일을 구체적으로 지정해 주는지?

> ⇨ 전국 단일의 공통업무와 관련된 개인정보파일은 중앙행정기관에서 '개인정보파일 표준목록'을 등록·관리하고, 각 지방자치단체·교육기관 등은 중앙행정기관이 제공하는 '개인정보 파일 표준목록'에 따라 개인정보파일을 등록하여야 함
> 다만, 중앙행정기관이 '개인정보파일 표준목록'을 따로 제공하지 않더라도 공공기관에서는 업무별로 개인정보 파일을 각각 등록하여야 함

□ 기관마다 개인정보파일명이 달라도 상관없는지?

> ⇨ 개인정보파일의 명칭은 공공기관에서 실제로 사용하는 업무단위를 근거로 작성하므로, 기관마다 등록하는 개인정보파일의 명칭이 달라도 상관없음

6 영향평가기관 지정기준 정비 (법 제33조)

1. 개정 개요

□ 개인정보 영향평가기관의 지정취소 근거가 시행령에서 법률에 상향됨에 따라 관련 규정을 정비하고,

○ 영향평가서 구성 항목 정비 및 요약본 공개 규정 신설 등 개인정보 영향평가 제도의 실효적 운영을 위해 일부 규정을 개선하였다.

2. 법령

법률	**제33조(개인정보 영향평가)** ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다. ② 보호위원회는 대통령령으로 정하는 인력·설비 및 그 밖에 필요한 요건을 갖춘 자를 영향평가를 수행하는 기관(이하 "평가기관"이라 한다)으로 지정할 수 있으며, 공공기관의 장은 영향평가를 평가기관에 의뢰하여야 한다. ③ 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다. 1. 처리하는 개인정보의 수 2. 개인정보의 제3자 제공 여부 3. 정보주체의 권리를 해할 가능성 및 그 위험 정도 4. 그 밖에 대통령령으로 정한 사항 ④ 보호위원회는 제1항에 따라 제출받은 영향평가 결과에 대하여 의견을 제시할 수 있다. ⑤ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다. ⑥ 보호위원회는 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다. ⑦ 보호위원회는 제2항에 따라 지정된 평가기관이 다음 각 호의 어느 하나에 해당하는 경우에는 평가기관의 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 평가기관의 지정을 취소하여야 한다. 1. 거짓이나 그 밖의 부정한 방법으로 지정을 받은 경우 2. 지정된 평가기관 스스로 지정취소를 원하거나 폐업한 경우 3. 제2항에 따른 지정요건을 충족하지 못하게 된 경우 4. 고의 또는 중대한 과실로 영향평가 업무를 부실하게 수행하여 그 업무를 적정하게 수행할 수 없다고 인정되는 경우 5. 그 밖에 대통령령으로 정하는 사유에 해당하는 경우 ⑧ 보호위원회는 제7항에 따라 지정을 취소하는 경우에는 「행정절차법」에 따른 청문을 실시하여야 한다.

	⑨ 제1항에 따른 영향평가의 기준·방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다. ⑩ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다. ⑪ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.
시행령	**제35조(개인정보 영향평가의 대상)** 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. 1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일 2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일 3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일 4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다. **제36조(평가기관의 지정 및 지정취소)** ① 보호위원회는 법 제33조제2항에 따라 다음 각 호의 요건을 모두 갖춘 법인을 개인정보 영향평가기관(이하 "평가기관"이라 한다)으로 지정할 수 있다. 1. 최근 5년간 다음 각 목의 어느 하나에 해당하는 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상인 법인 가. 영향평가 업무 또는 이와 유사한 업무 나.「전자정부법」 제2조제13호에 따른 정보시스템(정보보호시스템을 포함한다)의 구축 업무 중 정보보호컨설팅 업무(전자적 침해행위에 대비하기 위한 정보시스템의 분석·평가와 이에 기초한 정보 보호 대책의 제시 업무를 말한다. 이하 같다) 다.「전자정부법」 제2조제14호에 따른 정보시스템 감리 업무 중 정보보호컨설팅 업무 라.「정보보호산업의 진흥에 관한 법률」 제2조제1항제2호에 따른 정보보호산업에 해당하는 업무 중 정보보호컨설팅 업무 마.「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무 2. 개인정보 영향평가와 관련된 분야에서의 업무 경력 등 보호위원회가 정하여 고시하는 자격을 갖춘 전문인력을 10명 이상 상시 고용하고 있는 법인 3. 다음 각 목의 사무실 및 설비를 갖춘 법인 가. 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실 나. 기록 및 자료의 안전한 관리를 위한 설비 ② 평가기관으로 지정받으려는 자는 보호위원회가 정하여 고시하는 평가기관 지정신청서에 다음 각 호의 서류를 첨부하여 보호위원회에 제출해야 한다. 1. 정관 2. 대표자의 성명 3. 제1항제2호에 따른 전문인력의 자격을 증명할 수 있는 서류 4. 그 밖에 보호위원회가 정하여 고시하는 서류 ③ 제2항에 따라 평가기관 지정신청서를 제출받은 보호위원회는「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 다음 각 호의 서류를 확인해야 한다. 다만, 신청인이 제2호의 확인에 동의하지 않는 경우에는 신청인에게 그 서류를 첨부하게 해야 한다. 1. 법인 등기사항증명서 2.「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(외국인인 경우만 해당한다) ④ 보호위원회는 제1항에 따라 평가기관을 지정한 경우에는 지체 없이 평가기관 지정서를 발급

	하고, 다음 각 호의 사항을 관보에 고시해야 한다. 고시된 사항이 변경된 경우에도 또한 같다. 1. 평가기관의 명칭·주소 및 전화번호와 대표자의 성명 2. 지정 시 조건을 붙이는 경우 그 조건의 내용 ⑤ 법 제33조제7항제5호에서 "대통령령으로 정하는 사유에 해당하는 경우"란 다음 각 호의 어느 하나에 해당하는 경우를 말한다. 1. 제6항에 따른 신고의무를 이행하지 않은 경우 2. 평가기관으로 지정된 날부터 2년 이상 계속하여 정당한 사유 없이 영향평가 실적이 없는 경우 3. 제38조제2항 각 호 외의 부분에 따른 영향평가서 등 영향평가 업무 수행 과정에서 알게 된 정보를 다른 사람에게 누설한 경우 4. 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우 ⑥ 제1항에 따라 지정된 평가기관은 지정된 후 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우에는 보호위원회가 정하여 고시하는 바에 따라 그 사유가 발생한 날부터 14일 이내에 보호위원회에 신고해야 한다. 다만, 제3호에 해당하는 경우에는 그 사유가 발생한 날부터 60일 이내에 신고해야 한다. 1. 제1항 각 호의 어느 하나에 해당하는 사항이 변경된 경우 2. 제4항제1호에 해당하는 사항이 변경된 경우 3. 평가기관을 양도·양수하거나 합병하는 등의 사유가 발생한 경우 **제37조(영향평가 시 고려사항)** 법 제33조제3항제4호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다. 1. 민감정보 또는 고유식별정보의 처리 여부 2. 개인정보 보유기간 **제38조(영향평가의 평가기준 등)** ① 법 제33조제9항에 따른 영향평가의 평가기준(이하 "평가기준"이라 한다)은 다음 각 호와 같다. 1. 해당 개인정보파일에 포함되는 개인정보의 종류·성질, 정보주체의 수 및 그에 따른 개인정보 침해의 가능성 2. 법 제23조제2항, 제24조제3항, 제24조의2제2항, 제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다) 및 제29조에 따른 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해의 가능성 3. 개인정보 침해의 위험요인별 조치 여부 4. 그 밖에 법 및 이 영에 따라 필요한 조치 또는 의무 위반 요소에 관한 사항 ② 법 제33조제2항에 따라 영향평가를 의뢰받은 평가기관은 평가기준에 따라 개인정보파일의 운용으로 인한 개인정보 침해의 위험요인을 분석·평가한 후 다음 각 호의 사항이 포함된 평가결과를 영향평가서로 작성하여 해당 공공기관의 장에게 보내야 하며, 공공기관의 장은 제35조 각 호에 해당하는 개인정보파일을 운용 또는 변경하기 전에 그 영향평가서를 보호위원회에 제출해야 한다. 1. 영향평가의 대상 및 범위 2. 평가 분야 및 항목 3. 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가 4. 제3호의 분석·평가 결과에 따라 조치한 내용 및 개선계획 5. 영향평가의 결과 6. 제1호부터 제5호까지의 사항에 대하여 요약한 내용 ③ 보호위원회 또는 공공기관의 장은 제2항제6호에 따른 영향평가서 요약 내용을 공개할 수 있다. ④ 보호위원회는 법 및 이 영에서 정한 사항 외에 평가기관의 지정 및 영향평가의 절차 등에 관한 세부 기준을 정하여 고시할 수 있다.

3. 개정내용 해설

1. 영향평가기관의 지정 및 지정취소

□ 보호위원회는 다음 각 호의 모든 요건을 갖춘 법인을 영향평가기관으로 지정할 수 있으며, 시행령 제36조 제1항의 지정 요건 중 제2호의 전문인력 요건의 경우 영 별표1의2에서 규정하던 것을 개인정보 영향평가에 관한 고시 별표1에서 규정하는 것으로 개정하였다.

< 영향평가기관 지정요건(영 제36조제1항) >

1. 최근 5년간 다음 각 목의 어느 하나에 해당하는 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상인 법인
   가. 영향평가 업무 또는 이와 유사한 업무
   나.「전자정부법」 제2조제13호에 따른 정보시스템(정보보호시스템을 포함한다)의 구축 업무 중 정보보호컨설팅 업무(전자적 침해행위에 대비하기 위한 정보시스템의 분석·평가와 이에 기초한 정보 보호 대책의 제시 업무를 말한다. 이하 같다)
   다.「전자정부법」 제2조제14호에 따른 정보시스템 감리 업무 중 정보보호컨설팅 업무
   라.「정보보호산업의 진흥에 관한 법률」 제2조제1항제2호에 따른 정보보호산업에 해당하는 업무 중 정보보호컨설팅 업무
   마.「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무
2. 개인정보 영향평가와 관련된 분야에서의 업무 경력 등 보호위원회가 정하여 고시하는 자격을 갖춘 전문인력을 10명 이상 상시 고용하고 있는 법인
3. 다음 각 목의 사무실 및 설비를 갖춘 법인
   가. 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실
   나. 기록 및 자료의 안전한 관리를 위한 설비

○ 평가기관이 보유해야 하는 전문인력은 일반수행인력과 고급수행인력으로 구분되며, 일반수행인력 자격요건 중「개인정보 보호법」 제32조의2 제7항에 따른 인증심사원 자격을 취득한 사람의 경우 별도의 개인정보 영향평가 관련 분야 수행 경력이 없어도 자격 기준을 갖춘 것으로 인정하도록 개정하였다.

< 영향평가 전문인력 자격기준(고시 제5조, 별표1) >

<일반수행인력>

1.「국가기술자격법」에 따른 정보통신 직무분야의 국가기술자격 중 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 전자계산기조직응용기사, 정보처리기사, 정보보안기사 또는 정보통신기사 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
2.「전자정부법」 제60조에 따른 감리원(ISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
3. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

4. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
5. 「개인정보 보호법」 제32조의2제7항에 따른 심사원 자격을 취득한 사람
6. 한국CPO포럼이 시행하는 개인정보관리사 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야 수행실적이 있는 사람

<고급수행인력>

1. 일반수행인력의 자격을 갖춘 후 5년 이상의 영향평가 관련 분야 수행 실적이 있는 사람
2. 관련 분야 박사학위를 취득한 후 3년 이상의 영향평가 관련 분야 수행 실적이 있는 사람
3. 「국가기술자격법 시행규칙」 제3조에 따른 정보관리기술사·컴퓨터시스템응용기술사·정보통신기술사 자격을 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람

□ 보호위원회는 영향평가기관이 다음 각 호의 어느 하나에 해당하는 경우 지정을 취소할 수 있으며, 다만 제1호 또는 제2호에 해당하는 경우 평가기관 지정을 취소하여야 하며,

○ 평가기관으로 지정된 날로부터 2년 이상 영향평가 실적이 없거나, 영향평가 업무 수행 과정에서 알게 된 정보를 다른 사람에게 누설한 경우에도 평가기관 지정을 취소할 수 있도록 지정 취소 사유를 신설하였다.

< 개인정보 영향평가기관 지정취소 사유 >

1. 거짓이나 그 밖의 부정한 방법으로 지정을 받은 경우
2. 지정된 평가기관 스스로 지정취소를 원하거나 폐업한 경우
3. 제2항에 따른 지정요건을 충족하지 못하게 된 경우
4. 고의 또는 중대한 과실로 영향평가업무를 부실하게 수행하여 그 업무를 적정하게 수행할 수 없다고 인정되는 경우
5. 개인정보 보호법 시행령 제36조제6항에 따른 신고의무를 이행하지 않은 경우
6. 평가기관으로 지정된 날부터 2년 이상 계속하여 정당한 사유 없이 영향평가 실적이 없는 경우
7. 개인정보 보호법 시행령 제38조제2항 각 호 외의 부분에 따른 영향평가서 등 영향평가 업무 수행 과정에서 알게 된 정보를 다른 사람에게 누설한 경우
8. 그 밖에 개인정보 보호법 또는 개인정보 보호법 시행령에 따른 의무를 위반한 경우

2. 개인정보 영향평가 수행 절차 및 방법

□ 공공기관이 시행령 제35조 각 호에 해당하는 개인정보 파일을 운용 또는 변경하려는 경우에는 개인정보 영향평가를 수행하여야 한다.

< 영향평가 대상 개인정보파일(영 제35조) >

1. 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일 : 구축·운용 또는 변경하려는 개인정보파일에 5만명 이상의 정보주체에 관한 개인정보가 포함된 경우
2. 다른 개인정보파일과 연계하려는 경우 : 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계한 결과 50만명 이상의 정보주체에 관한 개인정보가 포함된 경우
3. 일반적인 개인정보 파일 : 구축·운용 또는 변경하려는 개인정보파일에 100만명 이상의 정보주체에 관한 개인정보가 포함된 경우
4. 영향평가를 받은 후 개인정보 검색 체계 등 개인정보파일의 운용 체계를 변경하려는 경우 : 해당 개인정보파일 중 변경된 부분

□ 영향평가 수행 대상에 해당하는 경우 영향평가 대상기관은 다음과 같이 사전 준비, 영향평가 수행, 이행 단계로 영향평가를 수행해야 한다.

① (사전 준비) 영향평가 대상기관은 사업계획서 작성 및 예산 확보 등을 거쳐 영향평가를 수행할 영향평가기관을 선정해야 한다.

② (영향평가 수행) 영향평가를 의뢰받은 영향평가기관은 영향평가 수행 후 영향평가서를 해당 공공기관의 장에게 보내야 하며, 영향평가서의 구성 항목은 다음과 같다.

< 영향평가서 구성 항목(영 제38조제2항) >

1. 영향평가의 대상 및 범위
2. 평가 분야 및 항목
3. 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가
4. 제3호의 분석·평가 결과에 따라 조치한 내용 및 개선계획
5. 영향평가의 결과
6. 제1호부터 제5호까지의 사항에 대하여 요약한 내용

③ (영향평가 이행) 영향평가서를 받은 공공기관의 장은 영향평가서를 제출받은 날로부터 1년 이내에 개선사항 이행 현황을 보호위원회에 제출해야 한다.

④ (요약본 공개) 보호위원회 또는 공공기관의 장은 영 제38조 제2항 제6호에 따른 영향평가서를 요약한 내용을 공개할 수 있다.

○ 다만, 정보공개법에 따른 비공개 대상 정보가 있는 경우 요약본의 일부 또는 전부를 공개하지 않을 수 있으며, 비공개 대상에 해당하는 지 여부는 각 기관에서 관련 규정 등에 따라 엄격히 판단하여 그 공개 여부를 결정해야 한다.

< 비공개 사유 예시 >

- 개인정보 파일 및 개인정보 처리 시스템 자체 또는 요약본 구성 항목 중 일부가 법률 상 비밀이나 비공개 사항으로 규정된 경우
- 개인정보 파일 및 개인정보 처리 시스템 자체 또는 요약본 구성 항목 중 일부가 국가안보·국방·통일·외교관계 등에 관한 것으로, 공개될 경우 국가의 중대한 이익을 현저히 해칠 우려가 있다고 인정되는 경우

- 개인정보 파일 및 개인정보 처리 시스템 자체 또는 요약본 구성 항목 중 일부가 공개될 경우 국민의 생명·신체 및 재산의 보호에 현저한 지장을 초래할 우려가 있다고 인정되는 정보
- 의사결정 과정 또는 내부검토 과정에 있는 사항 등으로서, 공개될 경우 업무의 공정한 수행이나 연구·개발에 현저한 지장을 초래한다고 인정할만한 상당한 이유가 있는 정보. 다만, 이 경우 영향평가 대상 파일 및 시스템의 운용을 시작하고 최대 1개월 이내에 요약본 공개 권장
- 기타 정보공개법 상 비공개 대상 정보에 해당하는 경우

□ 영향평가 대상이 되는 개인정보의 처리 근거가 법령에 규정되어 있어 정보주체가 그 대략적인 처리 내용을 예측할 수 있거나,

○ 개인정보파일 처리 시스템 구축·변경 또는 영향평가 사업 추진 시 그 개인정보 처리에 관한 사업 개요 및 내용이 조달 시스템(나라장터 등) 등을 통해 공개되는 경우 영향평가 요약본을 공개할 것을 권장하며,

○ 영향평가서를 요약한 내용을 공개하는 경우 개인정보파일의 운용 또는 변경 시점에 각 기관 홈페이지를 통해 공개해야 한다.

◈ 보다 자세한 사항은 「개인정보 영향평가 수행안내서」를 통해 안내 예정(~'24.1월)

4. 개인정보처리자 유의사항

□ 법 개정 이전에는 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보는 법 제33조를 적용하지 않아 개인정보 영향평가를 수행하지 않았으나,

○ 법 개정으로 「통계법」에 따라 수집되는 개인정보인 경우에도 시행령 제35조의 영향평가 대상 개인정보파일에 해당하는 경우에는 개인정보 영향평가를 수행하여야 한다.(법 시행일 '23.9.15.부터 2년 이내 영향평가를 실시하고 그 결과를 보호위원회에 제출)

5. 제재 규정

위반행위	제재 내용
제33조제1항을 위반하여 영향평가를 하지 아니하거나 그 결과를 보호위원회에 제출하지 아니한 자	3천만원 이하의 과태료 (제75조제2항제16호)

* 부칙 규정에 따라 공포 후 1년이 경과한 날('24.3.15)부터 과태료 부과 가능

6. 질의 응답

□ 법 제32조에 따라 개인정보 파일의 등록 및 공개 예외 사유에 해당하는 경우에도 개인정보 영향평가를 수행하여야 하는지? 또한 이 경우에 영향평가서를 요약한 내용을 공개하여야 하는지?

⇨ 개인정보 파일의 등록 및 공개 여부와 관계없이 개인정보 보호법 시행령 제35조에 따라 영향평가 대상이 되는 개인정보파일을 처리하는 경우에는 개인정보 영향평가를 수행하여야 함

⇨ 마찬가지로, 개인정보 파일의 등록 및 공개 예외 대상인 경우라도, 영향평가서를 제출받은 공공기관의 장은 그 요약본을 공개할 수 있음(영향평가서 구성항목 중 정보공개법 제9조의 비공개대상 정보에 해당하는 사항은 비공개 가능)

※ 개인정보 보호법 제32조에 따른 개인정보 파일 등록 및 공개 제도는 정보주체의 열람청구 등을 지원하기 위한 제도로, 파일 등록과 별개로 개인정보 보호법 제35조에 따른 열람권은 보장됨

□ 법 개정으로 영향평가 수행 의무가 부과된 '「통계법」에 따라 수집되는 개인정보'는 무엇인지?

⇨ 「통계법」에 따라 수집되는 개인정보는 「통계법」 제17조에 따른 지정통계의 작성이나 제18조에 따른 통계청장의 승인을 받은 통계의 작성을 위하여 수집되는 개인정보로 한정함

결정례	「통계법」에 따라 승인을 받지 않은 통계작성을 위하여 제공받은 개인정보의 적용 제외에 해당 여부
「통계법」 제18조제1항에 따른 통계청장의 승인을 받지 아니한 장애인 관련 통계작성을 위하여 보건복지부로부터 장애인의 주민등록번호, 장애종류, 장애등급 정보를 제공받고자 할 경우, 위 정보는 「개인정보 보호법」 제58조제1항제1호에 정한 '「통계법」에 따라 수집되는 개인정보'에 해당하지 않으므로 개인정보 보호법 제3장부터 제8장까지의 적용이 제외되지 아니한다(보호위원회 결정 제2017-23-176호)	

□ 개인정보파일의 운용 또는 변경 전에 영향평가를 수행해야 한다면, 개인정보파일을 구축한 이후라도 운용 전에만 영향평가를 수행하면 되는지?

⇨ 영향평가 수행 시점이 '개인정보파일을 구축·운용 또는 변경하기 전'에서 '개인정보파일을 운용 또는 변경하기 전'으로 개정되었으므로, 개인정보파일을 구축한 이후라도 운용 전에 영향평가를 수행 가능

- 다만, 개인정보 처리 시스템의 구축 이전 설계 단계에서 개인정보 침해 위험요인을 사전에 분석하여 개선사항을 도출하려는 영향평가 제도 취지를 고려하여 개인정보 처리 시스템 또는 개인정보 파일 구축 이전에 영향평가를 수행하는 것을 권고

□ 영향평가를 미수행하거나 그 결과를 보호위원회에 제출하지 않는 경우 과태료 부과 대상인데, 법 시행일('23.9.15) 이전에 영향평가를 완료하지 않는 경우 과태료 부과를 받는지?

> ⇨ 부칙규정에 의해 영향평가에 대한 과태료 부과 규정(법 제75조제2항제16호)은 공포 후 1년이 경과한 날부터 시행하므로, '24.3.15 이후에도 영향평가를 미수행하거나, 그 결과를 보호위원회에 제출하지 않은 경우 과태료 부과 대상이 될 수 있음

□ 특정 개인정보처리 시스템에서 처리되는 개인정보파일이 여러개이고, 해당 파일을 합하면 주민등록번호가 5만건 이상 포함된 경우, 반드시 영향평가를 수행해야 하는지? 일부 주민등록번호가 중복되어 5만건 이상인 경우에도 영향평가를 해야 하는지?

> ⇨ 개인정보처리 시스템에서 여러개의 개인정보파일이 처리되는 경우, 5만명 이상의 정보주체에 관한 고유식별정보를 포함하는 파일에 대해서만 영향평가를 수행하면 됨
>
> - 다만 시스템에서 처리되는 개인정보파일이 현재 시점 기준으로 영향평가 의무 대상이 되는 양적 기준에 해당하지 않더라도, 개인정보 증가에 따라 가까운 시기(1년 이내)에 개인정보 보호법 제35조의 기준을 초과할 것이 확실한 경우 가급적 시스템 운용 시점에 해당 개인정보 파일에 대해 영향평가를 수행할 것을 권장

참고 **개인정보 영향평가에 관한 고시('23.10.16. 시행)**

제1장 총칙

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제33조와 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제37조, 제38조에 따른 평가기관의 지정 및 영향평가의 절차 등에 관한 세부기준을 정함을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음과 각 호와 같다.

1. "개인정보 영향평가(이하 "영향평가"라 한다)"란 법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
2. "대상기관"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관을 말한다.
3. "개인정보 영향평가기관(이하 "평가기관"이라 한다)"이란 영 제37조제1항 각 호의 요건을 모두 갖춘 법인으로서 공공기관의 영향평가를 수행하기 위하여 개인정보 보호위원회(이하 "보호위원회"라 한다)가 지정한 기관을 말한다.
4. "대상시스템"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템을 말한다.
5. "개인정보 영향평가 관련 분야 수행실적(이하 "영향평가 관련 분야 수행실적"이라 한다)"이란 영 제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

제2장 개인정보 영향평가기관의 지정

제3조(평가기관 지정절차) ① 영 제37조에 따른 평가기관의 지정절차는 지정신청 공고, 지정신청 서류 접수 및 검토, 현장실사, 종합심사의 순으로 진행된다.

② 보호위원회는 평가기관으로 지정받으려는 자가 지정 신청을 할 수 있도록 관보 등을 통해 15일 이상 지정신청공고를 하여야 한다.

③ 영 제37조제2항에 따라 평가기관으로 지정받으려는 자는 별지 제1호서식의 "개인정보 영향평가기관 지정신청서"와 함께 다음 각 호의 서류를 보호위원회에 제출한다.

1. 영 제37조제2항제1호부터 제3호까지의 규정에 따른 서류
2. 별지 제2호서식의 개인정보 영향평가 수행실적 명세서
3. 별지 제3호서식의 개인정보 영향평가 수행실적물 관리카드
4. 별지 제4호서식의 개인정보 영향평가 수행인력 보유현황
5. 별지 제5호서식의 개인정보 영향평가 수행인력의 경력 및 실적 증명서
6. 별지 제6호서식의 개인정보 영향평가 수행인력 관리카드
7. 별지 제7호서식의 개인정보 영향평가 수행능력 세부 심사자료
8. 별지 제8호서식의 개인정보 영향평가 관련 기술자산 보유목록
9. 별지 제9호서식의 개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황
10. 영 제37조제1항제1호의 사실을 증명할 수 있는 서류
11. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(영 제37조제3항 각 호 외의 부분 단서에 해당하는 경우에만 첨부한다)등 그 밖에 평가기관 지정을 위해 필요하다고 판단되는 서류

④ 보호위원회는 제3항에 따른 평가기관 지정신청을 받은 경우 지정기준의 적합여부를 심사하기 위하여 평가기관 지정심사위원회(이하 "지정심사위원회"라 한다)를 구성·운영한다.

⑤ 보호위원회는 지정심사위원회의 심사결과를 검증한 후 평가기관 지정을 확정하고, 별지 제10호서식의 개인정보 영향평가기관 지정서를 교부한다.

⑥ 평가기관의 유효기간은 보호위원회가 평가기관으로 지정한 날로부터 3년으로 한다.

⑦ 평가기관의 유효기간을 연장하고자 하는 자는 유효기간 만료일 3개월 전까지 제3조제3항에 따른 서류를 보호위원회에 제출해야 한다.

⑧ 영 제37조제6항에 따른 신고는 별지 제11호서식의 개인정보 영향평가기관 변경사항 신고서에 따른다.

제4조(지정심사위원회의 구성 및 운영) ① 제3조에 따른 지정심사위원회는 다음 각 호의 자격을 가진 자 중에서 보호위원회가 위촉하는 5인 이상 15인 이내의 위원으로 구성한다.

1. 「고등교육법」 제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 8년 이상인 사람
2. 개인정보 보호 관련 업체, 기관 또는 단체(협회, 조합)에서 8년 이상 개인정보 보호 업무에 종사한 사람
3. 그 밖에 개인정보 보호에 관한 학식과 경험이 풍부한 사람

② 지정심사위원회는 영 제37조제1항에 따른 신청한 법인의 자격 및 업무수행능력 등을 검토한다.

③ 지정심사위원회의 위원 임기는 3년으로 하되, 연임할 수 있다.

④ 지정심사위원회의 회의는 필요에 따라 보호위원회가 소집한다.

제5조(영향평가 수행인력 자격) ① 영향평가 수행인력은 다음 각 호와 같이 일반수행인력과 고급수행인력으로 구분할 수 있다.

1. 일반수행인력의 자격은 다음 각 목과 같다.
   가. 별표1에 따른 전문인력의 자격을 갖춘 사람
   나. 한국CPO포럼이 시행하는 개인정보관리사 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야 수행실적이 있는 사람
2. 고급수행인력의 자격은 다음 각 목과 같다.
   가. 제1호의 일반수행인력의 자격을 갖춘 후 5년 이상의 영향평가 관련 분야 수행실적이 있는 사람
   나. 관련 분야 박사학위를 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람
   다. 「국가기술자격법 시행규칙」 제3조에 따른 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사 자격을 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람

② 제1항에 따른 영향평가 수행인력은 제6조제2항에 따른 전문교육을 이수하고 제6조제3항에 따른 전문인력 인증서를 받은 경우에 영향평가를 수행할 수 있다.

제6조(영향평가 전문교육의 운영 및 실시) ① 보호위원회는 영향평가 전문인력 양성을 위한 세부 교육계획 수립 및 교육 운영 등의 업무를 효율적으로 추진하기 위하여 한국인터넷진흥원을 전문교육기관으로 지정한다.

② 전문교육기관의 장은 영향평가 전문인력 양성을 위한 세부 교육계획을 수립하여 전문교육 등을 실시하여야 한다.

③ 전문교육기관의 장은 전문교육 이수자에 대한 평가를 실시하고 그 결과에 따라 개인정보 영향평가 전문인력 인증서를 교부한다. 이 경우 인증서의 유효기간은 인증서를 교부받은 날로부터 3년으로 한다.

④ 전문교육기관의 장은 제3항에 따른 전문인력 인증서를 교부받은 날로부터 매 2년이 경과한 자에 대해 계속교육을 실시하여야 하며, 인증서를 교부받은 자는 자격 유지를 위해 인증서 유효기간 만료 전까지 계속교육을 이수하여야 한다.

⑤ 전문교육기관의 장은 제4항의 요건을 충족한 자에 한하여 제3항의 개인정보 영향평가 전문인력 인증서를 갱신하여 교부하고, 인증서의 유효기간을 인증서를 교부받은 날로부터 3년간 연장한다.

제7조(영향평가 수행능력심사의 세부평가 및 지정기준) ① 평가기관의 영향평가 수행능력심사의 세부평가기준은 별표 2와 같다.

② 보호위원회는 영향평가 수행능력심사 세부평가기준에 따른 심사결과가 총점 75점 이상인 경우 신청한 법인을 평가기관으로 지정한다.

③ 평가기관의 유효기간을 연장하고자 하는 자에 대한 세부평가기준은 별표 3과 같다.

제8조(사후관리) ① 보호위원회는 평가기관이 영 제37조제1항의 평가기관 지정요건을 충족하는 지 여부와 영 제37조제6항에 따른 변경사항을 확인하기 위하여 현장실사, 관련 자료제출 요구 등을 할 수 있다.

② 평가기관은 다음 각 호를 포함한 보호대책을 별표 4와 같이 수립·시행하여야 하며, 보호위원회는 그에 대한 준수여부를 점검할 수 있다.

1. 영향평가 수행구역 및 설비에 대한 보호대책
2. 영향평가 수행 인력에 대한 보호대책
3. 문서 및 전산자료에 대한 보호대책
4. 일반 관리적 보호대책

③ 보호위원회는 평가기관이 법 제33조제7항제3호부터 제5호까지의 규정에 해당하는 경우에는 지정취소 이전에 시정 및 보완을 요구할 수 있다.

제3장 개인정보 영향평가의 절차 등

제9조(평가절차) 대상기관은 다음 각 호와 같이 사전 준비, 영향평가 수행, 이행 단계로 영향평가를 수행한다.

1. 사전 준비 단계에서는 영향평가 사업계획을 수립하여 예산을 확보하고 평가기관을 선정한다.
2. 영향평가 수행 단계에서는 평가기관이 개인정보 침해요인을 분석하고 개선계획을 수립하여 영향평가서를 작성한다.
3. 이행 단계에서는 영향평가서의 침해요인에 대한 개선계획이 반영되는 가를 점검한다.

제9조의2(영향평가 수행) ① 개인정보파일을 구축·운용 또는 변경하고자 하는 공공기관의 장은 별표 5의 필요한 사항이 반영될 수 있도록 설계완료 전에 영향평가를 수행하여야 한다.

② 공공기관의 장이 개인정보파일을 구축·운용 또는 변경하고자 할 때에는 제1항의 영향평가 결과를 반영한 조치를 이행하고 그 결과를 보호위원회에 제출하여야 한다.

제9조의3(영향평가 개선계획 반영여부의 확인) 공공기관의 장은 개인정보 영향평가 수행 후, 영향평가 개선계획의 반영여부를 정보시스템 감리 시 확인하여야 한다. 단, 감리를 수행하지 않은 경우에는 정보시스템 테스트단계에서 영향평가 개선계획의 반영여부를 확인하여야 한다.

제10조(평가영역 및 평가분야) 영 제38조제1항의 영향평가기준에 따른 평가영역은 별표 5와 같다. 다만, 대상기관이 1년 이내에 다른 정보시스템의 영향평가를 받은 경우에는 대상기관의 개인정보 보호 관리체계에 대한 평가는 생략할 수 있다.

제11조(평가항목) ① 평가기관은 별표 5에 따라 적합한 평가항목을 선정하여 영향평가를 수행하여야 한다. 다만, 대상기관이 1년 이내에 이미 평가받은 항목은 그 변경이 없는 때에는 평가항목에서 제외된다.

② 별표 5에 명시되지 않은 특화된 IT기술을 적용하는 경우에는 해당 기술이 개인정보 보호에 미치는 영향에 대한 평가항목을 개발하여 영향평가 시 반영하여야 한다.

제12조(영향평가서의 제출) 영 제38조제2항에 따라 영향평가서를 제출받은 대상기관의 장은 2개월 이내에 평가결과에 대한 내부승인 절차를 거쳐 영향평가서 및 그 요약본(요약본을 공개하려는 경우 해당 요약본을 포함한다)을 보호위원회에 제출하여야 한다.

제12조의2(영향평가서 요약본의 공개) ① 공공기관의 장은 영 제38조제3항에 따라 개인정보 영향평가서를 요약한 내용을 공개하는 경우 공공기관의 정보공개에 관한 법률 등에 따라 해당 기관의 홈페이지에 공개할 수 있다. 이 경우 보호위원회는 공공기관의 장이 공개한 영향평가 요약본을 보호위원회가 구축하는 인터넷 사이트에 공개할 수 있다.

② 보호위원회는 공공기관의 영향평가 요약본 공개 실태에 대해 점검할 수 있으며, 점검 결과 필요한 경우 공공기관에 개선을 요청할 수 있다.

제13조(영향평가 수행안내서) 보호위원회는 영향평가에 필요한 세부기준 및 절차, 평가항목 등을 구체화하는 "영향평가 수행안내서"를 마련하여 제공할 수 있다.

제14조(영향평가 개선사항 이행) 영 제38조제2항에 따라 영향평가서를 제출받은 공공기관의 장은 개선사항으로 지적된 부분에 대한 이행계획 등을 별지 제13호서식에 따라 영향평가서를 제출받은 날로부터 1년 이내에 보호위원회에 제출하여야 한다.

제15조(재검토 기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 10월 16일을 기준으로 매 3년이 되는 시점(매 3년째의 10월 15일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-10호, 2023. 10. 16.>

이 고시는 고시한 날부터 시행한다.

※ 별표 및 별지 서식은 국가법령정보센터(www.law.go.kr) 참조

⑦ 개인정보 파기 특례규정 삭제 〔법 제39조의6 삭제〕

1. 개정 개요

□ 기존 법 제39조의6의 규정에 따라 정보통신서비스 제공자등은 1년 동안 서비스 이용이 없는 이용자의 개인정보는 파기하거나 별도 분리하여 보관하도록 의무화하였으나,

○ 정보주체 또는 개인정보처리자의 의사와 무관*하게 서비스를 1년 동안 이용하지 않는 경우 의무적으로 파기 또는 별도 분리 보관하도록 한 유효기간제 규정에 대한 실효성 문제 등이 지속적으로 제기되었다.

* (예시) 코로나19 상황에서 해외 여행이 제한되어 면세점 홈페이지 서비스 이용이 1년 동안 없어서 파기 등의 조치를 하는 경우 이용자와 기업 모두 불편 발생

□ 이번 개정을 통해 정보통신서비스 제공자등에만 적용되던 법 제39조의6 파기에 대한 특례규정을 삭제하고 법 제21조 일반 파기 규정을 적용하도록 하였다.

2. 법령

법률	**제39조의6(개인정보의 파기에 대한 특례)** ① 정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다. 다만, 그 기간에 대하여 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우에는 그에 따른다. ② 정보통신서비스 제공자등은 제1항의 기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항을 전자우편 등 대통령령으로 정하는 방법으로 이용자에게 알려야 한다.
시행령	**제48조의5(개인정보의 파기 등에 관한 특례)** ① 정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제39조의6제1항의 기간 동안 이용하지 않는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리해야 한다. 다만, 법 제39조의6제1항 본문에 따른 기간(법 제39조의6제1항 단서에 따라 이용자의 요청에 따라 달리 정한 경우에는 그 기간을 말한다)이 경과한 경우로서 다른 법령에 따라 이용자의 개인정보를 보존해야 하는 경우에는 다른 법령에서 정한 보존기간이 경과할 때까지 다른 이용자의 개인정보와 분리하여 별도로 저장·관리해야 한다. ② 정보통신서비스 제공자등은 제1항에 따라 개인정보를 별도로 저장·관리하는 경우에는 법 또는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 해당 개인정보를 이용하거나 제공해서는 안 된다. ③ 법 제39조의6제2항에서 "개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다. 1. 개인정보를 파기하는 경우: 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 2. 다른 이용자의 개인정보와 분리하여 개인정보를 저장·관리하는 경우: 개인정보가 분리되어 저장·관리되는 사실, 기간 만료일 및 분리·저장되어 관리되는 개인정보의 항목 ④ 법 제39조의6제2항에서 "전자우편 등 대통령령으로 정하는 방법"이란 서면등의 방법을 말한다.

3. 개정내용 해설

□ 법 개정으로 1년 간 서비스를 이용하지 않은 이용자의 개인정보를 파기하거나 분리 보관해야 하는 제39조의6 개인정보의 파기에 대한 특례규정이 삭제됨에 따라,

○ 정보통신서비스 제공자등에게만 별도로 부여되던 정보주체의 미이용 기간에 따른 개인정보 파기 의무사항은 없어지게 되며,

○ 모든 개인정보처리자는 동일하게 법 제21조 개인정보의 파기 규정에 따라 보유기간의 경과, 개인정보의 처리 목적 달성 등 개인정보의 파기 사유가 발생하였을 때 지체 없이 파기하여야 하며, 다른 법령에 따라 보존하는 경우 분리하여 저장·관리하도록 하는 일반규정의 적용을 받게 된다.

□ 이에 따라, 제39조의6에 따라 분리 보관하고 있던 개인정보에 대해서는 당초 개인정보 수집·이용 목적 및 보유기간, 정보주체의 권리 보장, 서비스의 특성, 안전조치 수준 등을 고려하여 파기하거나 안전성 확보에 필요한 조치와 함께 복원하여 처리할 수 있다.

4. 개인정보처리자 유의사항

□ 유효기간제 규정 삭제는 정보주체와 개인정보처리자의 의사를 존중하여 개별 서비스의 특성에 맞게 휴면고객의 개인정보를 안전하게 관리하도록 한 것이므로, 개인정보처리자는 유효기간제가 폐지되더라도 제공하는 서비스 특성, 정보주체의 이용주기 등 개별적 상황을 고려하여 자율적으로 휴면정책 유지 여부를 정할 수 있다.

※ (예시) ①서비스 미이용 기준 기간 1년 → 서비스 특성에 맞는 기간으로 변경(예시: 6개월, 1년, 2년 등 기간을 선택), ②별도 분리 보관 → 서비스 이용고객의 개인정보와 통합 관리하되 휴면고객의 특성에 맞는 안전조치 방안 보완 등

□ 개인정보 휴면정책이 변경된 경우 이에 대해 가입자들에게 사전 안내해야 한다.

○ 특히 종전 유효기간제에 따라 별도로 분리하여 보관하고 있던 개인정보를 파기하거나 일반회원 데이터베이스(DB)와 통합 관리하려는 사항은 개인정보 정책에 중요한 변경이 발생한 것이므로 사전에 정보주체에게 알릴 필요가 있다.

□ 정보주체에게 알릴 때에는 해당 개인정보를 파기하는 것인지, 별도 분리하여 보관하던 개인정보를 통합하려는 것인지를 명확하게 기재하여 알리고, 정보주체가 이의를 제기할 수 있는 방법도 함께 알려야 한다.

○ 특히 「개인정보 보호법」 개정(유효기간제 폐지)으로 인해 휴면정책을 변경한다는 사실과 이에 따라 정보주체가 개인정보 파기 또는 서비스 계속 이용 여부를 선택할 수 있다는 사실을 명확히 알릴 필요가 있다.

○ 유의할 점은, 정책 변경사항 안내를 마케팅 또는 광고 목적으로 이용하는 것은 개인정보보호법(제22조, 홍보·판매 권유 별도 동의), 정보통신망법(제50조, 영리목적의 광고성 정보 전송) 등에 반할 소지가 있다는 점이다.

좋은 사례	잘못된 사례
◉ 2023년 9월 15일 개인정보 보호법 개정(개정전 제39조의6 삭제)에 따라 **회원 휴면정책이 변경**되어 안내드립니다. · 변경내용 : 휴면으로 분류되었던 회원계정은 **00월 00일부터 순차적으로 '일반회원'으로 전환**됩니다. · 이의제기 및 문의 : 일반회원으로 전환을 원하지 않고 회원탈퇴를 원하시거나 문의사항이 있으신 경우 **고객센터(☎0000-0000)**로 연락주시면 자세히 안내드리겠습니다.	◉ 2023년 9월 15일 개인정보 보호법 개정에 따라 **휴면정책이 폐지**되어 **고객님의 휴면 상태가 해지**되었음을 알려드립니다. · 다시 돌아오신 것을 환영하는 의미에서, 지금 **홈페이지에 접속 및 로그인**하시고 **서비스를 이용하시면 최대 50,000원 상당의 할인 쿠폰을 지급**해드립니다.

□ 일반회원과 휴면회원 데이터베이스(DB) 통합 정책으로 전환 시 주의해야 할 사항은 다음과 같다.

○ 첫째, 당초 회원가입 시 정보주체로부터 동의받은 내용과 현재의 서비스 내용 간에 변경된 사항이 있는 경우에는 반드시 변경된 사항에 대하여 추가적인 동의를 받아야 한다는 점에도 유의해야 한다.

○ 둘째, 마케팅을 위한 홍보를 위해 광고성 정보를 전송하려는 경우에는 정보주체로부터 마케팅 활용 동의와 함께 정보통신망법(제50조)에 따른 수신동의 절차를 거쳤는지 여부도 반드시 확인해야 한다. 또한, 약관법에 따라 서비스 이용약관에 유효기간제와 관련된 내용을 포함하여 운영하고 있는 경우에는 수정할 사항이 있는지 등을 확인해야 한다.

○ 셋째, 국세기본법, 전자상거래법 등 다른 법률에 따라 개인정보를 일정기간 이상 보관해야 하는 경우의 분리 보관 의무(개인정보보호법 제21조제3항)는 유효기간제와는 별개의 의무사항이므로 계속하여 분리 보관해야 한다는 점을 유의해야 한다.

○ 넷째, 분리 보관하고 있던 휴면회원의 개인정보를 통합한 후 운영하는 과정에서 개인정보 침해가 발생하지 않도록 휴면상태였던 고객에 대하여는 반드시 본인인지 여부를 확인하는 절차(휴대전화 본인확인, 전자우편 본인확인 등)를 마련하여 운영할 필요가 있다.

□ 인터넷서비스 이용자도 마찬가지로 오래전에 가입 후 이용하지 않는 서비스에서 유효기간제 폐지 관련 안내를 받은 경우에는, 해당 서비스에 접속하여 자신의 개인정보를 현행화하여 서비스를 이용하거나, 회원 탈퇴를 통해 개인정보처리자가 자신의 개인정보를 파기하도록 조치할 필요가 있다.

5. 제재 규정

□ 해당사항 없음

6. 질의 응답

□ 분리 보관하던 기존 휴면회원의 개인정보를 파기하거나 복원하려는 경우에 정보주체에게 통지해야 하는지?

⇨ 삭제되는 제39조의6의 파기 특례는 정보주체의 의사에 따른 분리보관이 아닌 '장기미이용'이라는 법적 요건에 따라 분리보관 되었던 것이므로, 기존에 분리 보관하던 개인정보를 파기하거나 복원하려는 경우에는 최소한 정보주체에게 바뀐 정책에 대해 알려주고 파기 또는 복원을 진행하는 것이 바람직함
다만, 안내 시 광고성 정보가 포함되지 않도록 유의해야 함(영리 목적의 광고성 정보를 전송하려고 할 때는 「정보통신망법」의 적용을 받으므로 해당 법 제50조에 따른 광고성 정보 수신 동의 등 의무를 준수해야 함)

※ 광고성 정보 전송에 대한 수신 동의 관련 내용은 '불법스팸 방지를 위한 정보통신망법 안내서(2020.7., 방송통신위원회)' 참고

□ 휴면정책 변경에 대해 정보주체에게 사전에 안내하였으나, 정보주체가 일정 기간 동안 이에 대해 동의 의사를 밝히지 않은 경우에는 변경된 정책을 적용해도 되는지?

⇨ 사전에 안내하도록 한 것은 정보주체에게 충분한 정보를 제공하도록 한 취지로, 동의 의사를 확인하도록 의무화한 것은 아님

참고 **표준 개인정보 보호지침('24.1.5. 시행 예정)**

제1장 총칙

제1조(목적) 이 지침은 「개인정보 보호법」(이하 "법"이라 한다) 제12조제1항에 따른 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
2. "개인정보처리자"란 업무를 목적으로 법 제2조제4호에 따른 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 모든 공공기관, 법인·단체, 개인 등을 말한다.
3. "공공기관"이란 법 제2조제6호 및 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제2조에 따른 기관을 말한다.
4. "친목단체"란 학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 각종 동창회, 동호회, 향우회, 반상회 및 동아리 등의 모임을 말한다.
5. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항 또는 제3항에 해당하는 자를 말한다.
6. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
7. "개인정보처리시스템"이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
8. "고정형 영상정보처리기기"란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 영 제3조제1항에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.

8의2. "이동형 영상정보처리기기"란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 영 제3조제2항에 따른 착용형, 휴대형, 부착·거치형 장치를 말한다.

9. "개인영상정보"란 법 제2조제1호에 따른 개인정보 중 고정형 영상정보처리기기 또는 이동형 영상정보처리기기에 의하여 촬영·처리되는 영상 형태의 개인정보를 말한다.
10. "고정형영상정보처리기기운영자"란 법 제25조제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하는 자를 말한다.

10의2. "이동형영상정보처리기기운영자"란 법 제25조의2제1항 각 호에 따라 업무를 목적으로 이동형 영상정보처리기기를 운영하는 자를 말한다.

11. "공개된 장소"란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

제3조(적용범위) 이 지침은 전자적 파일과 인쇄물, 서면 등 모든 형태의 개인정보파일을 운용하는 개인정보처리자에게 적용된다.

제4조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하

며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 기술적·관리적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.

⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제5조(다른 지침과의 관계) 중앙행정기관의 장이 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하는 경우에는 이 지침에 부합되도록 하여야 한다.

제2장 개인정보 처리 기준

제1절 개인정보의 처리

제6조(개인정보의 수집·이용) ① 개인정보의 “수집”이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 개인정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.

② 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체로부터 사전에 동의를 받은 경우
2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 그 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 공공기관이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
5. 개인정보를 수집·이용하지 않고는 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 곤란한 경우
6. 명백히 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
7. 개인정보처리자가 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다.
8. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

③ 개인정보처리자는 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 “명함등”이라 함)를 제공받음으로써 개인정보를 수집하는 경우 명함등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

④ 개인정보처리자는 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 “인터넷 홈페이지등”이라 함)에

서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

⑤ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집·이용할 수 있다.

⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」에 따른 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

제7조(개인정보의 제공) ① 개인정보의 "제공"이란 개인정보의 저장 매체나 개인정보가 담긴 출력물·책자 등을 물리적으로 이전하거나 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위를 말한다.

② 법 제17조의 "제3자"란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한한다)과 법 제26조제2항에 따른 수탁자는 제외한다(이하 같다).

③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제8조(개인정보의 목적 외 이용·제공) ① 개인정보처리자가 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.

② 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 자는 해당 개인정보를 제공받는 자와 개인정보의 안전성 확보 조치에 관한 책임관계를 명확히 하여야 한다.

③ 개인정보처리자가 법 제18조제3항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제9조(개인정보 수집 출처 등 통지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 법 제20조제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니 하다.

1. 통지를 요구하는 대상이 되는 개인정보가 법 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 통지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

② 개인정보처리자는 제1항 단서에 따라 제1항 전문에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제10조(개인정보의 파기방법 및 절차) ① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다.

② 영 제16조제1항제1호의 '복원이 불가능한 방법'이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.

③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.

⑤ 개인정보처리자 중 공공기관의 개인정보파일 파기에 관하여는 제55조 및 제56조를 적용한다.

제11조(법령에 따른 개인정보의 보존) ① 개인정보처리자가 법 제21조제1항 단서에 따라 법령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.

② 제1항에 따라 개인정보를 분리하여 저장·관리하는 경우에는 개인정보 처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장·관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.

제12조(동의를 받는 방법 등) ① 개인정보처리자가 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 법 제22조제1항에 따라 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

② 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 다음 각 호의 조건을 모두 충족해야 한다.

1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것
2. 동의를 받으려는 내용이 구체적이고 명확할 것
3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것
4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

③ 개인정보처리자는 법 제22조제1항 각 호의 어느 하나에 해당하는 경우에는 동의 사항을 구분하여 각각 동의를 받아야 한다.

1. 삭제
2. 삭제
3. 삭제
4. 삭제
5. 삭제

④ 개인정보처리자는 제3항에 해당하여 개인정보를 처리하고자 하는 경우에는 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.

⑤ 개인정보처리자는 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보처리방침에 공개하거나 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 “서면등의 방법”이라 한다)으로 정보주체에게 알려야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

⑥ 개인정보처리자가 영 제17조제2항제2호의 규정에 따라 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑦ 개인정보처리자가 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 정보주체의 동의 없이 개인정보를 수집·이용할 수 있다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 기타 친목단체의 구성원 상호 간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항

⑧ 개인정보처리자가 정보주체의 동의를 받기 위하여 동의서를 작성하는 경우에는 개인정보 처리 동의 안내서를 준수하여야 한다.

제13조(법정대리인의 동의) ① 영 제17조의2제1항에 따라 개인정보처리자가 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.

② 개인정보처리자는 법 제22조의2제2항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 한다.

제14조(정보주체의 사전 동의를 받을 수 없는 경우) 개인정보처리자가 법 제15조제1항제5호 및 법 제18조제2항제3호에 따라 정보주체의 사전 동의 없이 개인정보를 수집·이용 또는 제공한 경우 해당 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집·이용 또는 제공한 사실과 그 사유 및 이용내역을 알려야 한다.

제15조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

② 개인정보처리자는 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라 해당 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을 관리하기 위한 조치를 취해야 한다.

③ 개인정보처리자는 개인정보취급자에게 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

제2절 개인정보 처리의 위탁

제16조(수탁자의 선정 시 고려사항) 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자“라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자“라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등 개인정보 처리 및 보호 역량을 종합적으로 고려하여야 한다.

제17조(개인정보 보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적·기술적·물리적 조치를 하여야 한다.

제3절 개인정보 처리방침 작성

제18조(개인정보 처리방침의 작성기준 등) ① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 법 제30조제1항 각 호 및 영 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 개인정보처리자는 처리하는 개인정보가 개인정보의 처리 목적에 필요한 최소한이라는 점을 밝혀야 한다.

제19조(개인정보 처리방침의 기재사항) 개인정보처리자가 개인정보 처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다.

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
5. 영 제14조의2제2항에 따라 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우 같은 조 제1항 각 호의 고려사항에 대한 판단 기준(해당되는 경우에만 정한다)
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사

항(해당되는 경우에만 정한다)

7. 개인정보의 파기절차 및 파기방법(법 제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)

8. 법 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)

9. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)

10. 법 제28조의2 및 제28조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)

11. 영 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항

12. 개인정보 처리방침의 변경에 관한 사항

13. 법 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처

14. 법 제31조의2제1항에 따라 국내대리인을 지정하는 경우 국내대리인의 성명, 주소, 전화번호 및 전자우편 주소(해당되는 경우에만 정한다)

15. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항

16. 개인정보의 열람청구를 접수·처리하는 부서

17. 정보주체의 권익침해에 대한 구제방법

제20조(개인정보 처리방침의 공개) ① 개인정보처리자가 법 제30조제2항에 따라 개인정보 처리방침을 수립하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 “개인정보 처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 영 제31조제3항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다. 이 경우에도 “개인정보 처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

③ 개인정보처리자가 영 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제21조(개인정보 처리방침의 변경) 개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

제4절 개인정보 보호책임자

제22조(개인정보 보호책임자의 공개) ① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.

② 개인정보처리자는 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 이 경우 개인정보 보호책임자와 개인정보 보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있다.

제23조(개인정보 보호책임자의 교육) 영 제32조제4항에 따라 보호위원회가 개설 운영할 수 있는 개인정보 보호책임자에 대한 교육의 내용은 다음 각 호와 같다.

1. 개인정보 보호 관련 법령 및 제도의 내용
2. 법 제31조제3항 및 영 제32조제1항 각 호의 업무수행에 필요한 사항
3. 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항

제24조(교육계획의 수립 및 시행) ① 보호위원회는 매년 초 해당 연도 개인정보 보호책임자 교육계획을 수립하여 시행한다.

② 보호위원회는 제1항의 교육계획에 따라 개인정보 처리 및 보호에 관한 전문성을 갖춘 단체에 개인정보 보호책임자 교육을 실시하게 할 수 있다.

③ 보호위원회는 개인정보 보호책임자가 지리적·경제적 여건에 구애받지 않고 편리하게 교육을 받을 수 있는 여건 조성을 위해 노력하여야 한다.

제5절 개인정보 유출 통지 및 신고 등

제25조(개인정보의 유출등) 개인정보의 분실·도난·유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다.

제26조(유출등의 통지시기 및 항목) ① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 된 때에는 72시간 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다.

1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우

③ 개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출등이 발생한 사실
2. 제1항의 통지항목 중 확인된 사항

④ 개인정보처리자는 개인정보 유출등의 사고를 인지하지 못해 유출등의 사고가 발생한 시점으로부터 72시간 이내에 해당 정보주체에게 개인정보 유출등의 통지를 하지 아니한 경우에는 실제 유출등의 사고를 알게 된 시점을 입증하여야 한다.

제27조(유출등의 통지방법) ① 개인정보처리자는 정보주체에게 제26조제1항 각 호의 사항을 통지할 때에는 서면등의 방법을 통하여 정보주체에게 알려야 한다.

② 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 법 제34조제1항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 30일 이상 게시하여야 한다.

제28조(개인정보 유출등의 신고) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 제26조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 한국인터넷진흥원에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해

정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보, 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

② 제1항에 따른 신고는 별지 제1호서식에 따른 개인정보 유출등 신고서를 통하여 하여야 한다.

③ 개인정보처리자는 개인정보 포털(www.privacy.go.kr)을 통하여 유출등 신고를 할 수 있다.

④ 개인정보처리자는 제1항에 따른 신고를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.

제29조(개인정보 유출등 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출등 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출등 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출등 대응 매뉴얼에는 유출등 통지·조회 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출등에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제30조(개인정보 침해 사실의 신고 처리 등) ① 개인정보처리자의 개인정보 처리로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 사람은 법 제62조제2항에 따른 개인정보침해 신고센터에 침해 사실을 신고할 수 있다.

② 제1항에 따른 개인정보침해 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수·상담
2. 개인정보 침해 신고에 대한 사실 조사·확인 및 관계자의 의견 청취
3. 개인정보처리자에 대한 개인정보 침해 사실 안내 및 시정 유도
4. 사실 조사 결과가 정보주체의 권리 또는 이익 침해 사실이 없는 것으로 판단되는 경우 신고의 종결 처리
5. 법 제43조에 따른 개인정보 분쟁조정위원회 조정 안내 등을 통한 고충 해소 지원

제6절 정보주체의 권리 보장

제31조(개인정보 열람 연기 사유의 소멸) ① 개인정보처리자가 법 제35조제3항 후문에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 영 제41조제1항제4호의 규정에 따른 개인정보의 제3자 제공 현황의 열람청구를 받은 개인정보처리자는 국가안보에 긴요한 사안으로 법 제35조제4항제3호마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제32조(개인정보의 정정·삭제) ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정·삭제 요구가 법 제36조제1항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제33조(개인정보의 처리정지) ① 개인정보처리자가 정보주체로부터 법 제37조제1항에 따라 개인정보처리를 정지하도록 요구받은 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보 처리의 일부 또는 전부를 정지하여야 한다. 다만, 법 제37조제2항 단서에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제34조(권리행사의 방법 및 절차) ① 개인정보처리자는 정보주체가 법 제38조제1항에 따른 열람등요구를 하는 경우에는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다.

② 제1항의 규정은 영 제46조에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 영 제47조에 따른 수수료와 우송료의 정산에도 준용한다.

제3장 영상정보처리기기 설치·운영

제1절 총칙

제35조(적용범위) 이 장은 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 설치·운영하는 고정형 영상정보처리기기 또는 이동형 영상정보처리기기와 그 기기를 통하여 처리되는 개인영상정보를 대상으로 한다.

제2절 고정형 영상정보처리기기의 설치

제36조(고정형 영상정보처리기기 운영·관리 방침) ① 고정형영상정보처리기기운영자가 법 제25조제7항에 따라 고정형 영상정보처리기기 운영·관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

② 고정형영상정보처리기기운영자가 법 제30조에 따른 개인정보 처리방침을 정할 때 고정형 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 제1항에 따른 고정형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다.

제37조(관리책임자의 지정) ① 고정형영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 관리책임자를 지정하여야 한다.

② 제1항의 관리책임자는 법 제31조제3항에 따른 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

③ 법 제31조에 따른 개인정보 보호책임자는 관리책임자의 업무를 수행할 수 있다.

제38조(사전의견 수렴) 고정형 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 영

제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제39조(안내판의 설치) ① 고정형영상정보처리기기운영자는 정보주체가 고정형 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 법 제25조제4항 본문에 따라 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 연락처
4. 고정형 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

② 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 고정형영상정보처리기기운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

③ 공공기관의 장이 기관 내 또는 기관 간에 고정형 영상정보처리기기의 효율적 관리 및 정보 연계 등을 위해 용도별·지역별 고정형 영상정보처리기기를 물리적·관리적으로 통합하여 설치·운영(이하 '통합관리'라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제1항에 따른 안내판에 기재하여야 한다.

제3절 이동형 영상정보처리기기의 운영

제39조의2(이동형 영상정보처리기기의 촬영 사실 표시) ① 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판, 안내서면, 안내방송 또는 그 밖에 이에 준하는 수단이나 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 한다.

② 드론을 이용한 항공촬영 등 촬영 방법의 특성으로 인해 정보주체에게 촬영 사실을 알리기 어려운 경우에는 보호위원회가 이동형 영상정보처리기기의 촬영 사실 표시를 지원하기 위하여 구축·운영하는 인터넷 사이트에 촬영 사실 및 목적, 촬영 일시 및 장소 등의 사항을 공지하는 방법으로 알릴 수 있다.

제39조의3(이동형 영상정보처리기기 운영·관리 방침) ① 이동형영상정보처리기기운영자는 법 제25조의2제4항에 따라 영 제25조제1항을 준용하여 다음 각 호의 사항이 포함된 이동형 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

1. 이동형 영상정보처리기기의 운영 근거 및 운영 목적
2. 이동형 영상정보처리기기의 운영 대수
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
5. 이동형영상정보처리기기운영자의 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 이동형 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

② 이동형영상정보처리기기운영자가 제1항에 따라 이동형 영상정보처리기기 운영·관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

③ 이동형영상정보처리기기운영자가 법 제30조에 따른 개인정보 처리방침을 정할 때 이동형 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 제1항에 따른 이동형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다.

제4절 개인영상정보의 처리

제40조(개인영상정보 이용·제3자 제공 등 제한 등) 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나

제3자에게 제공하여서는 아니 된다. 다만 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체에게 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 필요한 경우로서 법 제28조의2 또는 제28조의3에 따라 가명처리한 경우
5. 개인영상정보를 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
10. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

제41조(보관 및 파기) ① 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 고정형영상정보처리기기 또는 이동형 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 경과하거나 개인영상정보의 처리 목적 달성, 법 제2조제1호에 따른 가명정보의 처리 기간 경과 등 그 개인영상정보가 불필요하게 되었을 때에는 지체 없이 그 개인영상정보를 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 고정형영상정보처리기기운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제42조(이용·제3자 제공·파기의 기록 및 관리) ① 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정해져 있는 경우에는 그 기간
6. 이용 또는 제공의 형태
7. 이용 또는 제공한 개인영상정보의 업무처리 담당자

② 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
3. 개인영상정보 파기 담당자

제43조(영상정보처리기기 설치 및 운영 등의 위탁) ① 고정형영상정보처리기기운영자가 영 제26조제1항에 따라 고정형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 영 제24조에 따른 안내판 및 영 제27조에 따른 고정

형 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개하여야 한다.

② 이동형영상정보처리기기운영자가 법 제25조의2제4항에 따라 영 제26조를 준용하여 이동형 영상정보처리기기의 운영에 관한 사무를 제3자에게 위탁하는 경우에는 제39조의2에 따른 이동형 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개하여야 한다.

③ 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 영 제26조제1항에 따라 고정형 영상정보처리기기 또는 이동형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다.

제5절 개인영상정보의 열람등 요구

제44조(정보주체의 열람등 요구) ① 정보주체는 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 “열람등”이라 한다)을 해당 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보에 한한다.

② 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 공공기관인 경우에는 해당 기관의 장에게 별지 제2호서식에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.

③ 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 제1항에 따른 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 이때에 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.

④ 제3항의 규정에도 불구하고 법 제35조제4항 각 호의 어느 하나에 해당하는 경우에는 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 제한하거나 거부할 수 있다. 이 경우 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 10일 이내에 서면 등으로 제한 또는 거부 사유를 정보주체에게 통지하여야 한다.

1. 삭제
2. 삭제
3. 삭제

⑤ 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 제3항 및 제4항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.

1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람등의 목적
4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유
6. 개인영상정보 열람등의 업무처리 담당자

⑥ 삭제

제45조(개인영상정보 관리대장) 제42조제1항 및 제2항, 제44조제5항에 따른 기록 및 관리는 별지 제3호서식에 따른 ‘개인영상정보 관리대장’을 활용할 수 있다.

제46조(정보주체 이외의 자의 개인영상정보 보호) 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 제44조제2항에 따른 열람등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

제6절 개인영상정보 보호 조치

제47조(개인영상정보의 안전성 확보를 위한 조치) 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 개인영상정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 법 제29조 및 영 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행. 다만, 1만명 미만의 정보주체의 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장시 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제48조(개인영상정보처리기기의 설치·운영에 대한 점검) ① 공공기관의 장이 고정형 영상정보처리기기를 설치·운영하는 경우에는 이 지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 그 결과를 보호위원회에게 통보하고 영 제34조제3항에 따른 시스템에 등록하여야 한다. 이 경우 다음 각 호의 사항을 고려하여야 한다.

1. 고정형 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 고정형 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 고정형 영상정보처리기 설치·운영의 필요성 지속 여부 등

② 공공기관의 장은 제1항과 제3항에 따른 고정형 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.

③ 공공기관 외의 고정형영상정보처리기기운영자는 고정형 영상정보처리기기 설치·운영으로 인하여 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체점검 등 개인영상정보의 침해 방지를 위해 적극 노력하여야 한다.

제4장 공공기관 개인정보파일 등록·공개

제1절 총칙

제49조(적용대상) 이 장의 적용대상은 다음과 같다.

1. 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
2. 「국가인권위원회법」에 따른 국가인권위원회
3. 「공공기관의 운영에 관한 법률」에 따른 공공기관
4. 「지방공기업법」에 따른 지방공사 및 지방공단
5. 특별법에 의하여 설립된 특수법인
6. 「초·중등교육법」,「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교

제50조(적용제외) 이 장은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 관하여는 적용하지 아니한다.

1. 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속기관을 포함한다)에서 관리하는 개인정보파일

2. 법 제32조제2항에 따라 적용이 제외되는 다음 각목의 개인정보파일

가. 국가안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일

나. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국 관리에 관한 사항을 기록한 개인정보파일

다. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일

라. 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일

마. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일

바. 다른 법령에 따라 비밀로 분류된 개인정보파일

사. 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일

3. 법 제58조제1항제2호에 따라 적용이 제외되는 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일

가. 삭제

나. 삭제

다. 삭제

4. 영상정보처리기기를 통하여 처리되는 개인영상정보파일

5. 삭제

6.「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관이 금융업무 취급을 위해 보유하는 개인정보파일

제2절 개인정보파일의 등록주체와 절차

제51조(개인정보파일 등록 주체) ① 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 보호위원회에 등록하여야 한다.

② 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 보호위원회에 직접 등록하여야 한다.

③ 교육청 및 각급 학교 등은 교육부를 통하여 보호위원회에 등록하여야 한다.

④ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관을 통하여 보호위원회에 등록하여야 한다.

제52조(개인정보파일 등록 및 변경 신청) ① 개인정보파일을 운용하는 공공기관의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

② 개인정보파일 등록 신청 사항은 다음의 각 호와 같다. 신청은 「개인정보 처리 방법에 관한 고시」(이하 이 조에서 “고시”라 한다) 제3조제2항에 따른 별지 제2호서식의 ‘개인정보파일 등록·변경 등록 신청서’를 활용할 수 있다.

1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일의 명칭
3. 개인정보파일의 운영 근거 및 목적
4. 개인정보파일에 기록되는 개인정보의 항목
5. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
6. 개인정보의 처리 방법
7. 개인정보의 보유 기간
8. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서

10. 개인정보의 열람 요구를 접수·처리하는 부서

11. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유

12. 법 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과

③ 개인정보취급자는 등록한 사항이 변경된 경우에는 고시 제3조제2항에 따른 별지 제2호서식의 '개인정보파일 등록·변경등록 신청서'를 활용하여 개인정보 보호책임자에게 변경을 신청하여야 한다.

제53조(개인정보파일 등록 및 변경 확인) ① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 보호위원회에 등록하여야 한다.

② 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 보호위원회에 등록하여야 한다.

③ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 보호위원회에 등록하여야 한다.

④ 제1항부터 제3항의 등록은 60일 이내에 하여야 한다.

제54조(개인정보파일 표준목록 등록과 관리) ① 특별지방행정기관, 지방자치단체, 교육기관(학교 포함) 등 전국적으로 단일한 공통업무를 집행하고 있는 기관은 각 중앙행정기관에서 제공하는 '개인정보파일 표준목록'에 따라 등록해야 한다.

② 전국 단일의 공통업무와 관련된 개인정보파일 표준목록은 해당 중앙행정기관에서 등록·관리해야 한다.

제55조(개인정보파일의 파기) ① 공공기관은 개인정보파일의 보유기간 경과, 처리 목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 공공기관은 개인정보파일의 보유기간, 처리 목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 한다. 다만, 영 제30조제1항제1호에 따른 내부 관리계획이 수립되어 있는 경우에는 내부 관리계획에 개인정보 파기계획을 포함하여 시행할 수 있다.

③ 개인정보취급자는 보유기간 경과, 처리 목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, 별지 제4호서식에 따른 개인정보파일 파기요청서에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호책임자의 승인을 받아 개인정보를 파기하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 별지 제5호서식에 따른 개인정보파일 파기 관리대장을 작성하여야 한다.

제56조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제55조에 따라 개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체 없이 등록 사실을 삭제한 후 그 사실을 보호위원회에 통보한다.

제57조(등록·파기에 대한 개선권고) ① 공공기관의 개인정보 보호책임자는 제53조제1항에 따라 검토한 개인정보파일이 과다하게 운용되고 있다고 판단되는 경우에는 개선을 권고할 수 있다.

② 교육청 및 각급 학교, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관의 개인정보 보호책임자는 제53조제2항 및 제3항에 따라 검토한 개인정보파일이 과다하게 운용된다고 판단되거나, 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 개선을 권고할 수 있다.

③ 보호위원회는 개인정보파일의 등록사항과 그 내용을 검토하고 다음 각 호의 어느 하나에 해당되는 경우에는 법 제32조제3항에 따라 해당 공공기관의 개인정보 보호책임자에게 개선을 권고할 수 있다.

1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
2. 등록하지 않은 개인정보파일이 있는 경우
3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함하지 않은 경우
5. 기타 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우

④ 보호위원회는 제3항에 따라 개선을 권고한 경우에는 그 내용 및 결과에 대하여 보호위원회의 심의·의결을 거쳐 공표할 수 있다.

⑤ 보호위원회는 공공기관의 개인정보파일 등록·파기 현황에 대한 점검을 실시할 수 있다.

제3절 개인정보파일의 관리 및 공개

제58조(개인정보파일대장 작성) 공공기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

제59조(개인정보파일 이용·제공 관리) 공공기관은 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 별지 제6호서식의 '개인정보 목적 외 이용·제공대장'에 기록하여 관리해야 한다.

제60조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.

② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 다만, 보유기간은 별표 1의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과 「공공기록물 관리에 관한 법률 시행령」 제25조에 따른 기록관리기준표를 상회할 수 없다.

③ 삭제

제61조(개인정보파일 현황 공개 및 방법) ① 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 포함하여 관리해야 한다.

② 보호위원회는 개인정보파일 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개할 수 있다.

③ 보호위원회는 전 공공기관의 개인정보파일 등록 및 삭제 현황을 종합하여 매년 공개해야 하며, 개인정보파일 현황 공개에 관한 업무를 전자적으로 처리하기 위하여 정보시스템을 구축·운영할 수 있다.

제62조 삭제

제63조 삭제

부칙 <제2024-1호, 2024. 1. 5.(예정)>

이 고시는 고시한 날부터 시행한다.

※ 별표 및 별지 서식은 국가법령정보센터(www.law.go.kr) 참조