



법무법인(유) 세종

# 기업들이 반드시 점검해야 할 개정 개인정보보호법 핵심조항

2024. 6. 5. | 최광희 고문



**법무법인(유)세종**  
**최 광희 고문**  
**khchoi@shinkim.com**



### 고문

Shin & Kim · 정규직  
2024년 5월 - 현재 · 1개월  
대면근무



### 동부지검 사이버범죄중점수사 자문위원

동부지검 · 시간제  
2023년 6월 - 현재 · 1년



### 겸임교수

고려대학교(세종) · 시간제  
2023년 3월 - 현재 · 1년 3개월



### 방위산업기술보호위원

대한민국 국방부 · 시간제  
2023년 3월 - 현재 · 1년 3개월



### 부회장

한국정보보호학회 · 시간제  
2021년 1월 - 현재 · 3년 5개월



### Korea Internet & Security Agency

22년 5개월

### 사이버침해사고대응본부장

정규직  
2002년 1월 - 현재 · 22년 5개월  
대면근무

### 디지털보안산업본부장

정규직  
2021년 1월 - 2023년 1월 · 2년 1개월  
대한민국 서울 송파구

### 미래정책연구실장

2020년 1월 - 2021년 1월 · 1년 1개월

### 개인정보보호정책단장

2019년 1월 - 2020년 1월 · 1년 1개월



### LG U+ 침해사고 특별조사단 부단장

과학기술정보통신부 · 시즌  
2023년 1월 - 2023년 4월 · 4개월



### 행정관

청와대 국가안보실  
2017년 7월 - 2019년 1월 · 1년 7개월  
사이버안보비서관실



### Visiting Scholar

The George Washington University  
2014년 1월 - 2015년 2월 · 1년 2개월

# I.

## 개인정보보호법 개정 배경 및 방향

## I. 개인정보보호법 개정 배경과 방향

오피니언 > 동아광장

### ‘개망신법’ 국회 통과를 환영하며[동아광장/ 최재경]

동아일보 | 업데이트 2020-01-14 03:00

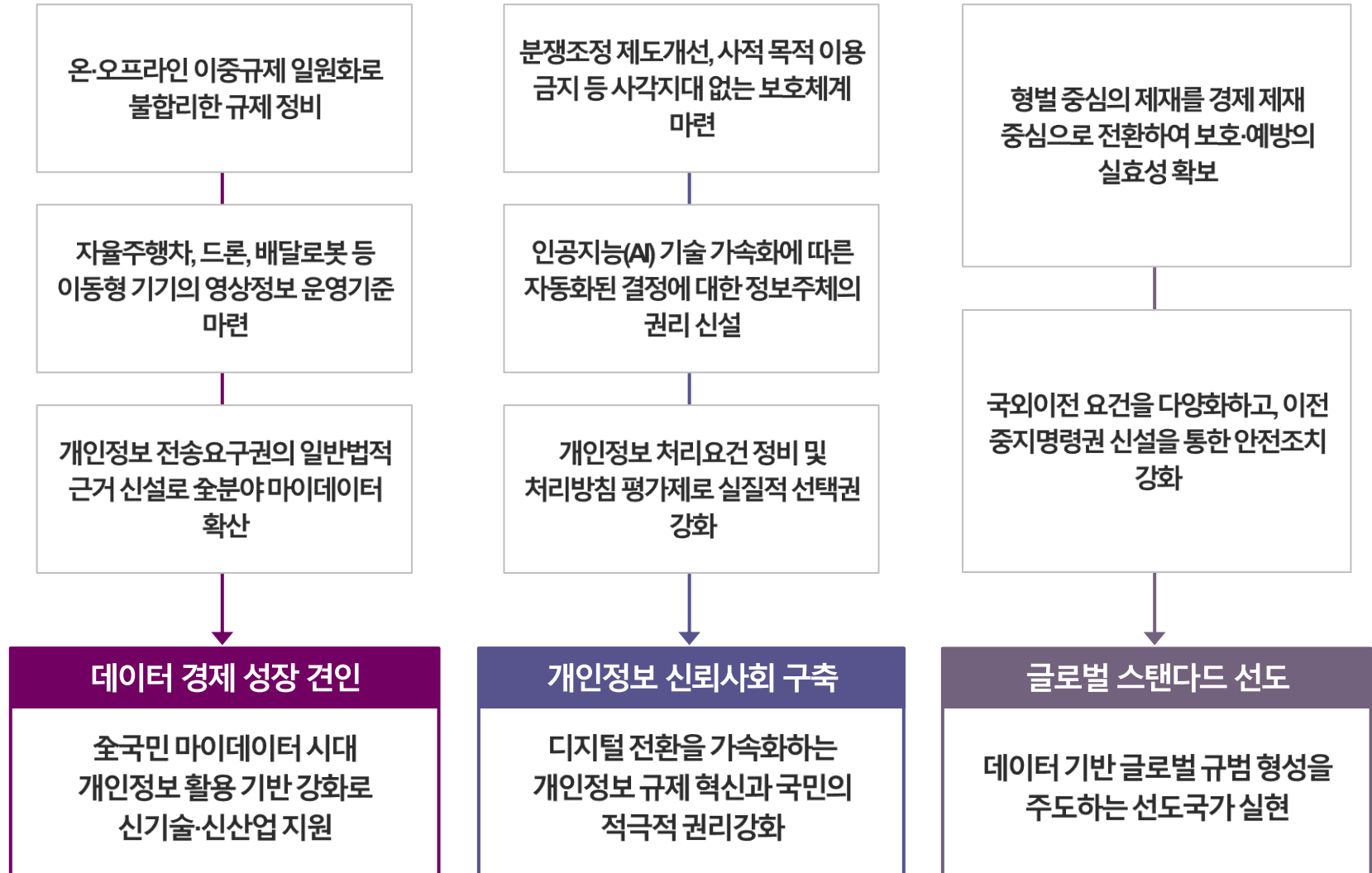
‘가명정보’ 활용 높인 ‘데이터 3법’, 의료-금융 등 이용 가능성 무한

규제 ‘대못’ 제거... 기업들 환영

7월부터 IT 관련 분야 빅뱅 예상

‘개인정보 돈벌이 수단’ 악용 없게 정보 보호 및 침해 처벌 강화 뒤따라야

# I. 개인정보보호법 개정 배경과 방향



# I. 개인정보보호법 개정 배경과 방향

개인정보 보호법 개정('23.3.14. 공포)에 따라 시행시기에 맞춰 1차('23.9.15.) 및 2차('24.3.15.) 후속 시행령 및 고시 등을 순차적으로 개정 완료

## 1차 시행

- 정보통신서비스특례정비, 이동형 영상기기 규정
- 동의 받는 방법 및 추가적인 이용제공
- 개인정보 처리방침 평가제, 분쟁조정제도 절차
- 공공시스템운영기관 특례 등 안전성 확보조치
- 국외 이전 및 중지 명령
- 과징금 부과기준, 공표명령 등

## 2차 시행

- 자동화된 결정에 대한 정보주체의 권리
- 개인정보 보호책임자의 업무 및 자격요건
- 공공기관 개인정보 보호 수준평가
- 손해배상의 보장 대상 범위 및 기준
- 개인정보 전송요구권 관련 규정

## II.

# 개인정보보호법 개정안 핵심사항

## II. 개인정보보호법 개정 핵심사항

### 1 이동형 영상정보처리기기 규정

#### ✓ 배경

- ◆ 기존 법은 고정형 영상기기(CCTV)만을 규율, 드론, 자율주행차, 로봇 등 이동형 영상정보처리기기의 특성에 맞는 기준으로는 미흡
  - ✓ 이동형 영상기기를 통한 개인정보 수집·이용 시 일반 규정이 적용되어 정보주체의 개별적 동의 필요

#### ✓ 개정내용

- ◆ 공개된 장소 등에서 **업무** 목적으로 이동형 영상정보처리기기를 이용하여 개인영상정보를 촬영하는 행위를 원칙적으로 제한
  - ✓ 개인정보 수집·이용 사유에 해당하거나, 정보주체가 촬영사실을 알 수 있었음에도 거부의를 밝히지 않은 경우 예외적으로 허용
  - ✓ 촬영을 하는 경우에는 불빛, 소리, 안내판, 서면, 안내방송 등으로 촬영 사실을 표시

#### 핵심

정보주체에게 촬영 사실을 알리기 어려운 경우, 보호위원회가 구축하는 인터넷 사이트에 공지



## II. 개인정보보호법 개정 핵심사항

### 2 온 오프라인 규제 일원화

#### ✓ 배경

- ◆ 데이터 3법 개정 시, 정보통신망법의 정보통신서비스 제공자 대상 규정을 특례(제6장)로 단순 이전·병합
  - ✓ 온·오프라인 서비스의 경계가 모호함에도 불구하고, 오프라인 규제(일반 규정)와 온라인 규제(특례 규정)의 이원화로 기업의 법 적용 혼선 및 이중 부담이 발생

#### ✓ 개정내용

- ◆ 특례 규정을 일반 규정과 일원화하여 모든 개인정보처리자 대상 '동일행위-동일규제' 원칙 적용
  - ✓ 유사·중복되는 특례 규정\*은 일반 규정으로 통합
  - ✓ 특례 규정에만 있는 손해배상 보장 제도, 국내 대리인 지정 제도, 개인정보 이용 내역 통지 등은 일반규정으로 전환하여 확대 적용

## II. 개인정보보호법 개정 핵심사항

### 2 온 오프라인 규제 일원화

#### 핵심 1 수집 출처 통지 및 이용·제공 내역 통지 제도 정비

- ◆ ‘수집 출처 통지 제도’와 ‘이용·제공 내역 통지 제도’ 운영의 일관성을 위해 개인정보 보유량 기준으로 일원화(5만명 이상 민감·고유식별정보, 100만명 이상 개인정보)
  - ✓ 수집 출처 통지와 ‘이용·제공 내역 통지’를 함께 통지

#### 핵심 2 안전성 확보 조치 중복 규정 일원화(영 제48조의2 삭제 → 영 제30조 통합)

- ◆ 안전조치를 위한 다양한 기술이 도입 될 수 있도록 규정을 기술 중립적으로 정비
  - ✓ 특정 기술에 한정된 침입탐지시스템, 비밀번호, 보안서버, 백신소프트웨어 등 문구 수정·삭제
  - ✓ 다양한 보안 기술이 적용될 수 있도록 개인정보의 전송·저장 시 암호화 기술 외에 ‘이에 상응하는 조치’ 허용
- ◆ 개인정보처리시스템의 개념 및 정의를 정비
  - ✓ 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템으로 변경

## II. 개인정보보호법 개정 핵심사항

### 2 온 오프라인 규제 일원화

#### 핵심 3 유출 통지 및 신고 중복 규정 일원화(영 제48조의4 삭제 → 영 제39조~제40조 통합)

- ◆ 개인정보가 유출되었다는 사실을 알게 된 경우 72시간 이내에 정보주체에게 통지하고, 개인정보위(또는 한국인터넷진흥원)에 신고
  - ✓ 유출 통지의 경우 정보주체의 연락처를 알 수 없는 경우 인터넷 홈페이지에 30일 이상 게시
- ◆ 신고 시 개인정보 유형, 유출 경로 및 규모 등을 고려하도록 규정
  - ✓ ① 1천명 이상의 정보주체 개인정보 유출, ② 민감정보·고유식별정보가 **1건 이상** 유출, ③ 외부로부터의 불법적인 접근(해킹)에 의해 **1건 이상** 유출 신고 대상으로 규정
  - ✓ 정보주체에 대한 유출 통지는 유출 규모와 관계없이 통지의무 이행



1건의 고유식별정보가 유출되었는데 연락처가 없어요  
홈페이지에 30일간 게시해야 하나요?

이용 중이신 통신사를 선택해 주세요.



☐ 전체 동의

☐ 개인정보이용 동의

☐ 서비스이용약관 동의

☐ 고유식별정보처리 동의

☐ 통신사이용약관 동의

## II. 개인정보보호법 개정 핵심사항

### 3 동의 제도 개선

#### ✓ 배경

- ◆ 사전동의 제도에 대한 과도한 의존으로 형식적 동의 및 '동의 만능주의' 관행 지속

#### ✓ 개정내용

- ◆ 동의 이외의 개인정보 적법 처리요건 활성화(제15조제4호 '불가피하게' 삭제)
  - ✓ 계약 체결·이행에 필요한 경우 수집·이용 활성화
- ◆ '정보주체의 자유로운 의사'에 따르도록 하는 등 동의 원칙을 구체화
  - ✓ ① 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것, ② 동의를 받으려는 내용이 구체적이고 명확할 것 ③ 쉽게 읽고 이해할 수 있는 문구를 사용할 것, ④ 동의 여부를 명확하게 표시할 수 있는 방법을 제공할 것 (시행일: 2024. 9. 15.)

#### 핵심

동의 없는 수집·이용에 대한 입증 책임은 개인정보처리자가 부담, 자유 의사를 보장

## II. 개인정보보호법 개정 핵심사항

### 4 개인정보 처리방침 평가제 도입

#### ✓ 배경

- ◆ 개인정보 처리에 관한 법정 고지 사항 등을 담은 '개인정보 처리방침'에 대한 내용의 적정성 및 구체성, 판단기준 미비 등 실체적 통제 미흡

#### ✓ 개정내용

- ◆ 개인정보 처리방침의 적정성을 평가하고 개선을 권고하여 국민의 권익을 보호할 수 있는 개인정보 처리방침 평가제 도입
  - ✓ 처리방침 작성지침 준수 여부, 정보주체가 이해하기 쉽게 작성하였는지 여부, 정보주체가 쉽게 확인할 수 있는 방법으로 공개하고 있는지 여부 등을 평가
  - ✓ 개인정보처리자의 유형 및 매출액 규모, 처리하는 개인정보의 유형·규모, 처리 근거 및 방식 등을 종합적으로 고려하여 평가 대상을 선정 할 수 있도록 규정 (령 제31조의2 신설)

#### 핵심

사고분야, 일방문자수, 매출액 등의 상위 기업이 대상

## II. 개인정보보호법 개정 핵심사항

### 5 개인정보 분쟁조정 제도 개선

#### ✓ 배경

- ◆ 조정신청 시 의무적으로 응해야 하는 기관은 공공기관에 한하며, 분쟁조정위에 사실 확인을 위한 조사권이 없어 적극적 조정에 한계

#### ✓ 개정내용

- ◆ 분쟁조정 요청 시, 의무적으로 응해야 하는 대상을 공공기관에서 모든 개인정보처리자로 확대
- ◆ 분쟁조정 관련 사실 확인이 필요한 경우 현장출입 및 자료조사 등 사실조사에 대한 법적근거를 명확히 규정
- ◆ 당사자가 조정안에 대한 수락 여부를 알리지 않을 경우 '거부'로 간주하던 것에서 '수락'으로 간주하는 것으로 기준 전환

## II. 개인정보보호법 개정 핵심사항

### 6 형벌 중심에서 경제제재 중심으로 전환

#### ✓ 배경

- ◆ 정보통신서비스 제공자에게만 적용되던 형벌규정을 일반규정에 맞추어 정비하고, 과도한 형벌규정은 삭제하는 대신 과징금 상한 및 대상 확대 등을 통해 실효성 확보

#### ✓ 개정내용

- ◆ 과징금 규정을 통합 정비하여 정보통신서비스 제공자에 적용되는 과징금을 개인정보처리자로 확대하고, 과징금 상한액 기준을 '위반행위 관련'에서 '전체 매출액' 3% 이하로 변경
  - ✓ 다만, 과징금 산정 시에는 위반행위에 상응하는 비례성과 효과성이 확보되도록 '위반행위와 관련 없는 매출액'은 제외

#### 핵심

#### 위반행위의 중대성 판단 기준

- |                            |                           |
|----------------------------|---------------------------|
| ① 위반행위의 내용 및 정도            | ② 암호화 등 안전성 확보 조치 이행 노력   |
| ③ 유출 등의 경우 위반행위와의 관련성 및 규모 | ④ 개인정보의 유형과 정보주체에게 미치는 영향 |
| ⑤ 위반행위로 인한 정보주체의 피해 규모     |                           |



제1조(목적) 이 법은 개인정보의 처리 및 보호에  
관한 사항을 정함으로써 개인의 자유와 권리를  
보호하고, 나아가 개인의 존엄과 가치를  
구현함을 목적으로 한다.

## II. 개인정보보호법 개정 핵심사항

### 7

#### 자동화된 결정에 대한 정보주체의 권리 도입 (법 제37조의2)

##### ✓ 배경

- ◆ 인공지능(AI) 등 신기술 발전에 따라 자동화된 결정(인사채용, 복지수급자 선정 등)이 광범위하게 활용되면서 새로운 프라이버시 이슈 제기

##### ✓ 개정내용

- ◆ 완전 자동화된 결정이 정보주체의 권리 또는 의무에 중대한 영향을 미치는 경우 정보주체에게 거부권, 설명 등 요구권 부여
- ◆ 개인정보처리자는 정보주체의 권리행사가 있으면 자동화 결정의 적용 배제, 인적 개입에 의한 재처리, 설명 등 조치 의무를 규정

## II. 개인정보보호법 개정 핵심사항

7

자동화된 결정에 대한 정보주체의 권리 도입 (법 제37조의2)

핵심 1

개인정보처리자의 조치 의무(영 제44조의3 신설)

- ◆ (자동화된 결정 거부 시) 해당 결정을 적용하지 않는 조치를 하고, 정보주체가 인적 개입에 의한 재처리를 요구한 경우 조치한 후 그 결과를 알려야 함
- ◆ (설명 요구 시) ①해당 결정의 결과, ②해당 결정에 사용된 주요 개인정보의 유형 및 영향 등을 포함하여, 간결하고 의미 있는 설명을 이해하기 쉽도록 제공

개별 설명 시  
포함해야 할 사항  
(영 §44의3②)

- ▶ 해당 자동화된 결정의 결과
- ▶ 해당 자동화된 결정에 사용된 주요 개인정보의 유형
- ▶ 개인정보의 유형이 자동화된 결정에 미친 영향 등 자동화된 결정의 주요 기준
- ▶ 해당 자동화된 결정에 사용된 주요 개인정보의 처리 과정 등 자동화된 결정이 이루어지는 절차

- ◆ (요구의 거절) 다른 사람의 생명·신체·재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 등 정당한 사유가 있는 경우 거절 가능(거절하는 경우 법 제38조제5항에 따라 그 사유를 지체 없이 알림)

## II. 개인정보보호법 개정 핵심사항

### 8 개인정보 보호책임자 전문성 및 독립성 강화 (법 제31조)

#### ✓ 배경

- ◆ CPO의 자격과 관련 그간 직위요건(예: 임원)만 규정하고 있고 전문성 및 독립성 요건은 미비하여 개인정보보호 전담인력으로서 실질적 역할수행에 한계

#### ✓ 개정내용

- ◆ 개인정보처리자에게 CPO가 업무를 독립적으로 수행할 수 있도록 보장할 의무를 부여

#### 핵심 1 개인정보 보호책임자(CPO)의 지정 및 자격요건(영 제32조 개정, 별표1 신설)

- ◆ 일정 기준 이상 개인정보처리자는 개인정보 보호 관련 일정 경력(자격요건)을 갖춘 전문성이 있는 CPO를 지정하도록 의무화
- ◆ 자격요건 : 개인정보보호 경력, 정보보호 경력, 정보기술 경력을 합하여 총 4년 이상 보유 (개인정보보호 경력 최소 2년 이상 필수)

## II. 개인정보보호법 개정 핵심사항

8

개인정보 보호책임자 전문성 및 독립성 강화 (법 제31조)

핵심 2

매출액, 개인정보의 보유 규모를 고려하여 일정기준 이상 개인정보처리자로 한정

### 자격요건을 갖춘 CPO 지정 의무대상

- ① 연간 매출액 또는 수입이 1,500억원 이상인 개인정보처리자로서,  
- 100만명 이상의 정보주체 개인정보 또는 5만명 이상의 민감정보·고유식별정보를 처리하는 자
- ② 전년도 말 기준 재학생(대학원 재학생 수를 포함) 수가 2만명 이상인 대학
- ③ 대규모 개인정보를 처리하는 상급종합병원
- ④ 보호위원회가 고시하는 기준을 충족하는 공공시스템운영기관

- ◆ 시행령 시행(2024.3.15.) 당시 지정되어 있는 CPO에 대하여는 2년 이내(2026.3.14.)에 자격요건을 갖추도록 경과조치 규정을 마련하고 준비기간을 부여하여 현장에서의 혼란을 최소화



# 감사합니다

---

**SHIN & KIM**  
법무법인(유) 세종

서울시 종로구 종로3길 17 디타워 D2 23층 (우)03155

[www.shinkim.com](http://www.shinkim.com)

T 02 316 4114

F 02 756 6226

본 자료에 대한 저작권 등 모든 권리는 법무법인세종 및 작성자에게 속하므로, 사전 허락 없이 본 자료를 사용, 복제, 배포, 활용하거나 다른 법률 사무소 등 제3자에게 제공하는 것은 엄격히 금지됩니다.