August 9, 2023

# 「개인정보의 안정성 확보조치 기준」 일부개정고시안 행정예고

개인정보보호위원회는 지난 2023. 7. 7.「개인정보의 안정성 확보조치 기준」 일부개정고시안(이하 "**개정안**")을 행정예고 한다고 밝혔습니다. 개정안은 개인정보 보호법 시행령에서 정보통신서비스제공자에게 적용되었던 특례규정 제48조의2(개인정보의 안전성 확보 조치에 관한 특례)가 일반규정인 제30조(개인정보의 안전성 확보조치)로 통합됨에 따른 후속조치로, 2023. 7. 26. 까지 의견 수렴 기간을 거쳐 8월 말 확정될 예정입니다. 개정안은 확정된 이후 개인정보 보호법 개정법률과 마찬가지로 2023. 9. 15. 부터 시행될 예정이며, 다만, 접근통제 관련 제6조 제2항, 개인정보 암호화 관련 제7조 제4항, 출력·복사시 안전조치 관련 제13조 제3항 및 제4항, 공공시스템운영기관 관련 제15조 내지 제18조 등 일부 규정은 공포 후 1년이 경과된 날부터 시행될 예정입니다.

개정안의 주요 내용은 다음과 같습니다.

## I. 주요내용

### 1. 「개인정보의 안정성 확보조치 기준」과 「개인정보의 기술적 · 관리적 보호조치 기준」 통합

기존 규제상으로는 개인정보처리자에 대해서는 일반규정인 「개인정보의 안정성 확보조치 기준」("**일반규정**")이 적용되고, 정보통신서비스제공자에 대해서는 특례규정인 「개인정보의 기술적 · 관리적 보호조치 기준」("**특례규정**")이 적용되어 개인정보 안전조치 기준이 이원화되어 있었습니다. 그러나 개인정보 보호법 개정 법률에서 수범자가 개인정보처리자로 일원화되고 정보통신서비스제공자에 적용되었던 특례규정 내용은 일반규정으로 통합됨에 따라 그간 이원화되어 있던 개인정보 안전조치 기준도 개정안으로 일원화됩니다.

### 2. 내부 관리계획 수립 · 시행 및 점검 (제4조)

개인정보처리자에게 내부 관리계획을 수립·시행하여야 할 의무를 부과하는 한편, 단서조항을 통하여 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 이를 생략할 수 있도록 하였습니다. 또한 개인정보처리자에게 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화된 교육을 정기적으로 실시하도록 하였습니다.

### 3. 개인정보처리시스템 접근 권한의 관리 (제5조)

개인정보처리자는 개인정보처리시스템에 대한 접근 권한과 관련하여 권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하고 최소 3년간 보관하도록 하였습니다(제3항). 개인정보처리자가 개인정보처리시스템에 접근할 수 있

는 계정을 발급하는 경우 개인정보취급자 별로 계정을 발급해야 하며, 동 계정이 다른 개인정보취급자와 공유되지 않도록 해야 하는 원칙은 유지하면서도 '정당한 사유'가 있는 경우 예외적으로 개인정보취급자 간 계정 공유가 허용될 수 있도록 단서가 추가되었습니다(제4항). 또한 기존 규제 하에서는 개인정보처리자 및 정보통신서비스제공자가 비밀번호 작성규칙을 수립하여야 하였다면, 개정안에서는 비밀번호 작성규칙 의무를 폐지하고, 대신 정보주체의 인증수단을 안전하게 적용 및 관리할 의무를 추가하였습니다. 이에 따라 사업자들은 다양한 인증수단을 도입할 수 있게 되었습니다(제5항).

## 4. 개인정보처리시스템 접근 통제 (제6조)

개정안에 특례규정이 통합되는 과정에서 기존 규제 하 정보통신서비스제공자의 망분리의무가 인터넷 망 차단 조치 의무로 용어 수정되었습니다. 이에 따라 개인정보처리자는 전년도 말 기준 직전 3개월 간 개인정보가 저장·관리되고 있는 '이용자' 수가 일일평균 100만명 이상인 경우 개인정보처리시스템에서 개인정보를 다운로드·파기할 수 있거나 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대해 인터넷망 차단 조치를 하여야 합니다. 다만, 개정안은 단서 조항에서 '클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 운영'하는 경우 해당 서비스 접속에 한하여 인터넷망 연결이 예외적으로 허용될 수 있도록 하였습니다(제6항).

## 5. 개인정보 암호화 (제7조)

개정안에서 일반규정과 특례규정이 통합됨에 따라 개인정보처리자가 암호화해야 할 정보 유형에 (기존 고유식별정보, 비밀번호, 생체인식정보에 더하여) '이용자'의 신용카드번호 및 계좌번호가 추가되었습니다. 이에 따라 개인정보처리자는 위 기재된 정보 모두를 안전한 암호 알고리즘으로 암호화하여 저장할 의무를 부담합니다. 또한 개인정보처리자가 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우 모든 개인정보를 암호화하도록 함으로써 암호화 대상이 변경되었습니다. 나아가, 10만 명 이상 개인정보를 보유한 대기업·중견기업·공공기관 또는 100만 명 이상 개인정보를 보유한 중소기업·단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위해 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수집 및 시행해야 합니다.

## 6. 접속기록 보관 및 점검 (제8조)

개인정보처리자가 개인정보처리시스템 접속기록을 보관하여야 하는 대상이 변경되었습니다. 개인정보처리자는 1) 개인정보처리시스템에 접속한 자(개인정보취급자 뿐만 아니라 이용자도 해당)의 접속기록을 3개월 이상, 2) 개인정보취급자의 접속기록을 1년 이상, 3) 정보주체 수 등 일정 조건을 충족하는 개인정보처리시스템에 접속하는 개인정보취급자의 접속기록을 2년 이상 보관 및 관리해야 합니다.

### 7. 악성프로그램 등 방지 (제9조)

개인정보처리자는 악성프로그램 등을 방지 치료할 수 있는 보안프로그램을 설치 운영하여야 하며 동 프로그램을 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지해야 합니다. 다만, 이번 개정안에서는 '정당한 사유'가 있는 경우 보안 프로그램 업데이트를 일정 기간 지연할 수 있도록 단서가 추가되었습니다.

### 8. 공공시스템운영기관의 안전조치 기준 도입 (제15조 내지 제18조)

공공시스템 지정 기준과 더불어 공공시스템운영기관인 공공기관이 준수해야 할 안전조치 기준이 신설되었습니다.

## II. 시사점

### 1. 개인정보 안전조치 의무 일원화

개정안은 일반 개인정보처리자와 정보통신서비스제공자등의 안전성 확보조치를 통합한다는 점에서 큰 의미가 있습니다. 다만, 이용자의 개념은 별도로 정의하고 있으며 이에 따라 이용자와 이용자가 아닌 정보주체를 구분하여 안전성 확보조치를 규정하고 있습니다.

### 2. 기술 발전 및 기술중립성 등을 고려한 안전조치 의무 준수 방법의 다양화

기술 발전 및 기술중립성, 안전조치 의무를 준수함에 있어 실질적인 보호조치, 실무상의 어려움 등을 종합적으로 고려하여 기존에 부과되었던 개인정보 안전조치 의무를 준수하는 방법이 보다 다양화되었습니다.

개인정보처리시스템에 접근할 수 있는 계정 발급과 관련하여 '정당한 사유'가 있는 경우 위 계정을 공유할 수 있도록 하고, 보안 프로그램의 업데이트를 지연할 수 있도록 하는 등 취급자별 계정 발급과 계정 공유 금지 원칙을 견지하면서도 개발 등 불가피한 경우를 감안하였습니다. 한편, 위 '정당한 사유'가 인정되기 위한 요건 등에 관하여는 향후 다양한 논의가 진행될 수 있을 것으로 보입니다(제5조 제4항).

한편, 비밀번호 작성규칙 대신 인증수단, 백신소프트웨어 대신 보안프로그램 등 보다 기술중립적인 단어를 사용하여 사업자가 필요한 경우 비밀번호 작성규칙, 백신소프트웨어 외에 다양한 보안수단을 활용할 수 있도록 여지를 마련했습니다(제5조 제5항).

개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에도 '자동으로 접속이 차단되도록 하는 등 필요한 조치'를 하여야 한다고 규정함으로써 접속 차단 외의 필요한 조치를 허용하였습니다(제6조 제4항).

인터넷 망 차단조치와 관련하여 클라우드컴퓨팅을 이용하여 개인정보처리시스템을 구성·운영하는 경우 해당 서비스 접속에 한하여 인터넷망 연결을 허용하였습니다(제6조 제6항). 이는 최근 클라우드컴퓨팅서비스를 통해 개인정

보를 처리하는 다수의 사업자를 고려하여 관련 의무를 현실화하려는 취지로 이해됩니다. 한편, 클라우드컴퓨팅서비스를 이용하지 않는 경우에는 개인정보를 다운로드 또는 파기할 수 있는 자에 대해 (그 정보의 양이나 내용에 상관없이) 인터넷망 차단 조치가 요구되는바 이를 준수함에는 다소의 애로사항이 있을 것으로 예상됩니다.

위에서 살펴본 새로운 보호조치에 대응하기 위해서는 일정한 시간이 소요될 수 있으므로, 개인정보처리자는 개인정보처리자의 관련 시스템을 식별하여 대상 시스템을 파악하고, 정보주체 및 이용자에 따른 의무를 사전에 확인하는 것은 물론, 그에 부합하는 적절한 보호조치를 마련할 수 있도록 사전에 준비해야 할 것으로 보입니다.

## 관련 구성원

**김도엽**
변호사
**T** 02.3404.0935
**E** doyeup.kim@bkl.co.kr

**이강혜**
변호사
**T** 02.3404.7454
**E** kanghye.lee@bkl.co.kr