

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」

개정(안) 주요 내용 I

- 개인정보보호, PIMS 등을 중심으로 -

2012. 3. 30(금)



Contents

I 추진 배경 및 경과

II 개정 방향

III 주요 내용

IV 향후 일정



I. 추진 배경 및 경과



1. 추진 배경

대량 개인정보 유출사고 빈발

- 최근 해킹을 통한 대규모 개인정보 유출 사고가 지속적으로 발생
 - ※ SK컴즈 3,500만명('11.7), 넥슨 1,320만명 ('11.11), 현대캐피탈 175만건 ('11.4)
- 유출된 개인정보를 이용한 스팸, 전화사기 등 2차 피해에 대한 국민 불안감 확산
 - ※ 개인정보 침해신고 건수 해마다 증가 ('07년 25,965→'10년 54,832→'11년 122,215, KISA)

개인정보 보호체계 강화 요구 증대

- 개인정보 유출 사고 재발 방지 및 2차 피해 예방을 위한 개인정보보호 체계 강화 필요
 - ※ 방송통신위, “인터넷상 개인정보보호 강화방안” 수립·추진 ('11.8)
- 정보통신망법 개정을 통해 기업의 개인정보 관리 의무를 강화하고,
이용자의 자기정보통제권을 보장 하기 위한 신규 제도 도입 ('12.8.18 시행)

2. 추진 경과

정보통신망법 및 시행령 개정 추진 경과

2011. 3월~11월 정보통신망법 개정(안) 7건 발의

2011. 12월 문방위 대안으로 국회 본회의 통과(12.29)

2012. 2월 정부 이송(2.3) 및 공포(2.17)

2012. 3월 개정 시행령(안) 입법예고 및 공청회 개최

2012. 6월~7월 개정 시행령 공포 (예정)

2012. 8월 개정 정보통신망법 시행(8.18)

※ 개인정보보호 관리체계 인증(PIMS)은 '13.2.18 시행



개정 정보통신망법에서 위임한 사항 및 세부 시행방안 마련을 위해
동법 **시행령 개정** 추진 중

II. 개정 방향



1. 개정 방향

기업의 개인정보 관리 강화

- 기업이 개인정보를 철저히 관리하도록 개인정보 보호조치 기준 상향
⇒ ①개인정보처리시스템과 외부 인터넷망 분리 (개정, 시행령 제15조제2항제3호)

과도한 개인정보 보관 제한

- 서비스 장기 미사용자 등의 불필요한 개인정보 보관 최소화
⇒ ②개인정보 유효기간제 도입 (신설, 법 제29조제2항, 시행령(안) 제15조의2)

이용자 자기정보결정권 강화

- 이용자가 개인정보의 활용 내역을 정확히 알고 통제할 수 있는 제도 마련
⇒ ③개인정보 이용내역 통지 제도 도입 (신설, 법 제30조의2, 시행령(안) 제15조의3)
- 개인정보 누출 시 이용자가 신속히 필요한 조치를 취함으로써 후속 피해 최소화
⇒ ④개인정보 누출 사고 통지·신고제 도입 (신설, 법 제27조의3, 시행령(안) 제14조의2)

개인정보보호 관리체계(PIMS) 인증 관련 규정 신설

- PIMS 인증 및 인증기관 운영에 관한 세부 기준 제공(절차, 방법, 범위 등)
⇒ 신설, 시행령 제47조, 제48조, 제50조~53조의5, 제54조의2

III. 주요 내용



1. 개인정보처리시스템과 외부 인터넷망 분리(1)

시행령(안) 개정 취지

- 최근 개인정보관리자 등의 계정 해킹에 의한 대량의 개인정보 유출사고가 발생함에 따라 사고를 예방하기 위한 높은 수준의 보안대책 마련 필요

시행령(안) 주요 내용

- **(적용 사업자)** 100만명 이상의 이용자 개인정보를 보유한 사업자는 업무망과 외부 인터넷망 분리 의무화
 - ※ 영향평가 대상이 되는 100만명 기준을 적용
- **(적용 대상)** 망분리 적용 사업자의 개인정보취급자는 망분리 대상
 - ※ 개인정보 DB 접근 및 저장 등의 권한을 가진 개인정보취급자로 범위 한정
- **(망분리 방법)** 물리적 망분리 뿐만 아니라 논리적 망분리도 허용
 - ※ 일정 수준의 보안성을 갖추었다면 논리적 망분리도 허용

2. 개인정보 누출 등의 통지·신고제 (1)

입법 취지

- 개인정보 누출사고 발생 시 이용자에게 해당 사실을 통지하고 방송통신위에 신고하여 명의도용, 금전적 피해 등 추가 피해 확산 방지

법 주요 내용

- **개인정보 분실·도난·누출(“누출 등”) 사실을 안 때, 지체 없이 이용자 통지 및 방통위 신고**
※ 누출 통지·신고제는 개인정보 누출등에 대해 이용자와 사업자, 정부가 신속히 대응하여, 2차 피해확산을 방지하는 것이 목적이므로 **누출 규모와 관계 없이 통지·신고**
- (통지·신고 내용) ①누출 개인정보 항목, ②누출 발생 시점, ③이용자가 취할 수 있는 조치, ④정보통신서비스 제공자등의 대응 조치, ⑤이용자 상담 접수 부서 및 연락처
- 개인정보의 누출등에 대한 대책 마련 및 피해 최소화 조치 강구
⇒ (시행령 위임) 통지갈음 조치, 통지·신고 방법 및 절차 등에 관하여 필요한 사항

2. 개인정보 누출 등의 통지 · 신고제 (2)

시행령(안) 주요내용

- (통지·신고 방법) 전자우편, 서면, 모사전송, 전화 또는 이와 유사한 방법
 - ※ (개인정보보호법) 정보주체에 대한 통지 및 조치결과 신고(1만명 이상 유출 시, 5일 이내 신고)
 - (정보통신망법) 누출 사실 인지 시 지체 없이 통지·신고하므로 내용과 방법이 동일 (조치결과 신고 아님)
- (통지에 갈음하는 조치) 인터넷 홈페이지에 30일 이상 게시
 - ※ 홈페이지 게시 곤란 시, 전국을 보급지역으로 하는 둘 이상의 일반 일간신문에 1회 이상 공고
- (통지·신고 절차) 개인정보 누출등 사실을 안 때 지체 없이 통지·신고
 - 단, 누출 개인정보 항목 및 발생 시점 미 확인 시, 확인된 사항 먼저 통지 후 추가 확인 사항 즉시 통지
 - ※ 확인 사항 우선 통지 시 이용자·사업자 조치 사항, 이용자 상담접수 부서·연락처는 함께 통지
 - ※ 판례상 “지체 없이”의 의미 : 합리적인 이유 및 근거가 없는 한 즉시

3. 개인정보 유효기간제 (1)

입법 취지

- 장기간 서비스를 이용하지 않는 이용자의 개인정보에 대해 파기 등 필요한 조치를 취함으로써 사업자가 불필요하게 보관하는 개인정보 최소화

법 주요 내용

- **대통령령이 정하는 기간** 동안 정보통신서비스를 이용하지 않은 이용자의 개인정보에 대해 **대통령령이 정하는 바에 따라 파기 등 필요한 조치**
⇒ (시행령 위임) 정보통신서비스를 이용하지 않은 기간(유효기간)의 기준,
파기 등 필요한 조치의 내용

3. 개인정보 유효기간제 (2)

시행령(안) 주요내용

- **(유효 기간)** 개인정보 파기등의 조치를 취할 수 있는 서비스 미이용기간은 **3년**으로 함
 - **(예외 ①)** 다른 법령 또는 계약(이용약관 등)으로 별도의 보존기간을 정한 경우
 - ※ 예) 전자상거래 소비자 보호법 : 소비자의 불만 또는 분쟁처리에 관한 기록 5년,
신용정보보호법 : 신용정보 업무처리에 관한 기록 3년, 의료법 : 환자명부 등 5년
 - **(예외 ②)** 법령상 책임 또는 의무 준수를 위하여 불가피한 경우
 - ※ 예) 국세기본법 : 국세 부과 제척기간 10년, 상법 : 상사채권 소멸시효 5년 등
- **(조치 사항)** 유효기간(3년)경과 후, 즉시 파기 또는 다른 개인정보와 분리 저장·관리
 - ※ 분리 저장·관리 시, 이용자가 요구하는 경우를 제외하고는 해당 정보를 이용·제공할 수 없음
- **(파기 대상)** 이용자로부터 최초로 수집한 개인정보에 한 함
 - ※ 이용자가 작성한 게시물, 쿠키 등 2차 생성물 제외
- **(통지 시기·내용)** 유효기간 도래 30일전까지, 파기 또는 분리 저장·관리 사실, 일시 및 해당 개인정보의 항목 통지

4. 개인정보 이용내역 통지제 (1)

입법 취지

- 사업자가 주기적으로 이용자의 개인정보 이용내역을 통지함으로써, 이용자는 본인의 개인정보 이용내역을 정확히 알고 통제 가능

법 주요 내용

- 대통령령이 정하는 정보통신서비스 제공자등은 **이용자 개인정보의 이용내역 (개인정보 취급위탁 및 제3자 제공 포함)**을 주기적으로 통지하여야 함
 - ※ 정보통신망법 제22조 및 제23조제1항단서에 따라 수집한 이용자 개인정보에 한 함
 - ※ 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 않은 경우는 예외
- ⇒ (시행령 위임) 대통령령이 정하는 기준에 해당하는 자, 통지하여야 하는 정보의 종류, 통지주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항

4. 개인정보 이용내역 통지제 (2)

시행령(안) 주요내용

- (적용 대상) 100만명 이상 이용자 개인정보 보유 정보통신서비스 제공자등
- (통지 정보의 종류) ① 개인정보 수집·이용목적 및 수집 항목, ②개인정보를 제공받은 자, ③제공 목적 및 제공 항목, ④취급 위탁 받은 자 및 취급위탁 목적
※ 이용자가 자신이 제공한 개인정보가 무엇이고, 무슨 목적으로 수집·이용되었는지 알아야 정확히 자기정보를 통제할 수 있으므로, 수집·이용 목적 및 항목 통지
- (통지 방법·주기) 전자우편·서면·모사전송·전화 등의 방법으로, 연 1회 이상 통지

5. 개인정보보호 관리체계 인증제도(PIMS) (1)

입법 취지

- PIMS 인증제도 법적 근거 마련을 통한 인증제도 활성화 기반 마련
- ※ 현재, PIMS는 방송통신위원회 의결(제2010-66-274호)을 근거로 운영중

법 주요 내용

- **(PIMS 인증 및 인증기준)** 방송통신위원회는 개인정보보호 관리체계를 수립·운영하고 있는 자에 대해 인증심사 기준에 적합한지 여부를 인증할 수 있음
 - PIMS 인증 업무 수행기관, 사후관리, 인증 내용 표시 및 홍보, 인증취소 등 제반 사항은 ISMS 규정을 준용토록 함
- ⇒ (시행령 위임) 인증방법, 절차, 범위, 수수료, 사후관리 방법, 절차, 인증취소 방법, 절차, 인증기관 지정의 기준, 절차, 유효기간 등

5. 개인정보보호 관리체계 인증제도(PIMS) (2)

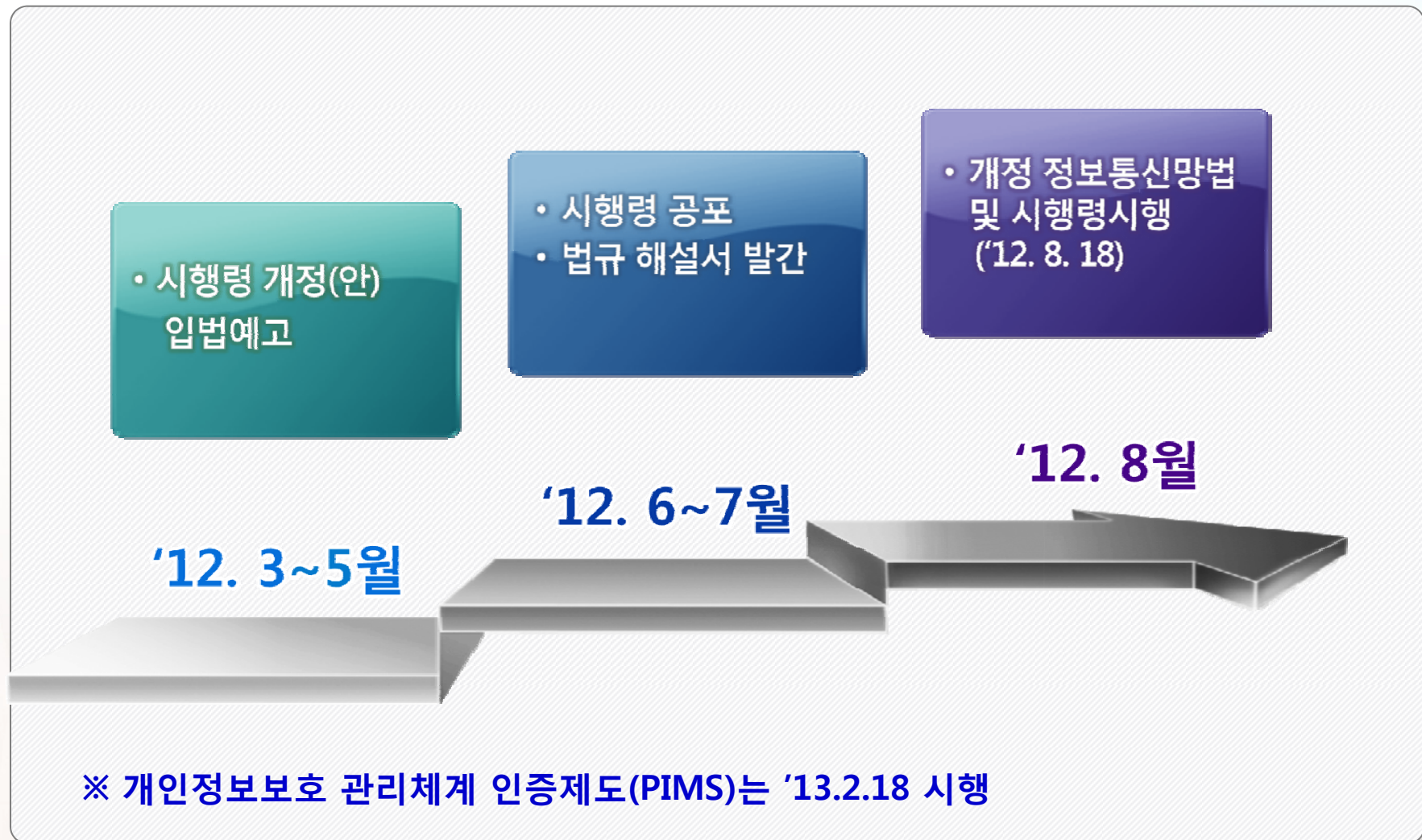
시행령(안) 주요내용

- (개인정보보호 관리체계 인증 방법·절차·범위 등) 인증신청 기관과 인증범위 및 일정 등 협의에 따라 서면 및 현장심사 실시 후 인증서 발급
- (인증 수수료) 인증 수수료 산정을 위한 구체적 기준을 고시하도록 규정
- (인증 업무 범위) KISA 또는 개인정보보호 관리체계 인증기관이 수행할 수 있는 '인증에 관한 업무 범위' 정의(인증기관이 업무 범위 중 전부 또는 일부를 수행할 수 있도록 함)
- (인증 취소 방법 및 절차) 인증 취소 시 서면으로 통지
- (인증 기관 지정 기준) 인증심사원 5명 이상 보유 및 방통위가 실시하는 업무수행 요건·능력 심사에서 적합 인정을 받아야 함
- (인증 기관 지정절차) 지정 신청서 수령 및 지정 기준 충족 여부 심사 수행
- (인증 기관 유효기간 및 사후관리) 지정 유효기간은 3년이며 인증실적 보고서 제출 요

V. 향후 계획



향후 추진일정



감사합니다

