Privacy Report 2020.11

SOMANSA

2020.11.13 개인정보보호위원회

개인정보보호법고시 〈개인정보의 안전성 확보조치 기준〉 고시 통합 개정안 사전공개

개정안 원문보기

고시개정배경

2020년 1월
데이터 3법 (개인정보보호법, 신용정보법, 정보통신망법)개정으로 인한
개인정보보호법과 정보통신망법 개인정보 관련규정 통합에 따라 고시 개정안 필요

주요변화

개정방향 정보통신망법고시에 포함된 규정을 개인정보보호법고시에 추가

주요변화항목

1. 망분리 요건 포함

2. 암호화 대상 확대

· 고유식별정보(주민, 여권, 운전면허, 외국인등록), 바이오정보, 비밀번호 + (추가) 신용카드번호, 계좌번호

3. 내부망과 DMZ 구분폐지로 인한 암호화 대상 확대

· 내부망과 DMZ 등 저장위치 상관없이 암호화
· 기존 개보법고시는 주민번호 이외 개인정보는 내부망 암호화 선택 사항으로 규정

4. 출력물 보안조치 강화

· 망법고시 9조 출력물 보안조치가 개보법고시로 이동
· 출력용도 특정 및 출력항목 최소화
· 종이인쇄물, 개인정보파일이 포함된 외부저장매체 관리조치구축

5. 개인정보 마스킹

· 개인정보조회, 출력업무 수행시 개인정보 마스킹하여 표시제한
· 망법고시 14조 개인정보 표시제한조치가 개보법고시로 이동

개인정보보호법고시
개인정보의 안전성 확보조치 고시 개정안 분석 (20.11.13 공개)

20.11.13 공개 개보법고시 | 20.8.11 시행 개보법고시 | 20.1.2 시행 망법고시

조항	키워드	개정고시	기존 개보법고시	기존 망법고시	차이점	기술적 보호조치
1조 목적	고시목적	① 안전성 확보에 필요한 최소한의 기준 설정	1조 명시	1조 ①항 명시	변동없음 개인정보보호법고시규정 유지	
		② 개인정보처리자 (정보통신서비스 제공자 포함)의 경우 처리하는 개인정보 보유수, 유형, 중요도 등 현황을 고려하여 스스로의 환경에 맞는 필요한 조치를 적용	-	1조 ②항 명시	망법고시 1조 ②항 추가	
2조 정의	용어정의	1. 개인정보처리시스템 2. 내부관리계획 3. 정보통신망 4. 비밀번호 5. P2P 6. 공유설정 7. 공개된 무선망 8. 모바일기기 9. 관리용단말기 10. 바이오인식정보 11. 보조저장매체 12. 접속기록 13. 인증정보	정보주체 및 기업기관 정의 등을 포함하여 20개 정의	내부관리계획, 망분리, P2P, 공유설정, 인증정보 포함하여 14개 정의	(추가) 내부관리계획, 정보통신망, P2P, 공유설정, 인증정보 (삭제) 정보주체, 개인정보파일, 대기업, 중견기업, 중소기업, 소상공인, 개인정보보호책임자, 개인정보취급자 (변동사항) 바이오정보 :얼굴, 홍채, 정맥, 음성, 필적 등 신체적 또는 행동적 특징→ 바이오인식정보: 개인의 신체적, 생리적, 행동적 특정에 관한 정보	
3조 안전조치 기준 적용	안전조치 적용대상	규모에 따라 차등적용	3조 명시	언급없음	변동없음 개인정보보호법고시규정 유지	
4조 내부관리 계획의 수립시행	관리적 조치	① 개인정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 않도록 내부의사결정 절차를 통하여 각 호의 사항을 포함하는 내부관리계획 수립 및 시행 1. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항 2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항 3. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 4. 위험 분석 및 관리에 관한 사항 5. 개인정보취급자에 대한 교육에 관한 사항 6. 접근 권한의 관리에 관한 사항 7. 접근 통제에 관한 사항 8. 개인정보의 암호화 조치에 관한 사항 9. 접속기록 보관 및 점검에 관한 사항 10. 악성프로그램 등 방지에 관한 사항 11. 물리적 안전조치에 관한 사항 12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항 13. 재해 및 재난 대비 개인정보처리시스템의 안전조치에 관한 사항 14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 15. 개인정보 내부관리계획의 수립, 변경 및 승인 절차에 관한 사항 16. 그 밖에 개인정보 보호를 위하여 필요한 사항	-	3조 ①항 3호 개인정보 내부관리계획의 수립 및 승인에 관한 사항 명시	망법고시 3조 ①항 3호 개인정보 내부관리계획의 수립 및 승인에 관한 사항이 개보법고시 4조 ①항 15호로 이동	개인정보보호 컨설팅
	개인정보교육	② 개인정보처리자는 아래 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시 1. 교육목적 및 대상 2. 교육 내용 3. 교육 일정 및 방법	-	3조 ②항 개인정보보호 관련 교육 실시	망법고시 3조 ②항 개인정보 교육관련 규정이 개보법고시 4조 ②항으로 이동	
5조 접근권한의 관리	인증수단	⑤ 비밀번호 이외의 인증수단을 적용하는 경우 안전한 인증 방법 적용	5조 ① 개인정보처리시스템 접근권한 차등부여 ② 개인정보 취급자 변동시 지체없이 변경말소 ③ 권한부여/변경말소 기록 최소 3년 보관 ④ 취급자별 사용자 계정 발급 ⑤ 비밀번호 작성규칙 수립 ⑥ 일정횟수 이상 인증실패시 접근제한	4조 접근통제 조항 ① 필요한 자에게만 부여 ② 개인정보 취급자 변동시 지체없이 변경말소 ③ 권한부여/변경말소 기록 최소 5년 보관 ④ 외부에서 개인정보처리시스템에 접속시 안전한 인증 수단 적용	개보법고시 5조 ⑤항 비밀번호 이외 인증 수단을 적용하는 경우 **'안전한 인증방법 적용' 신설** 망법고시 4조 ③항 권한부여/변경말소 기록3년 보관으로 축소	DB DLP DB 접근제어

조항	키워드	개정고시	기존 개보법고시	기존 망법고시	차이점	기술적 보호조치
6조 접근통제	개인정보 유출통제	③ 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통하여 열람권한 없는 자에게 공개/유출되지 않도록 개인정보처리시스템, **개인정보취급자의 컴퓨터** 및 모바일기기 등에 접근통제 조치	6조 ③항 개인정보처리시스템, **업무용 컴퓨터,** 모바일기기, **관리용 단말기** 접근통제 조치 구축	4조 ⑨항 홈페이지, P2P, 공유설정 등을 통해 유출되지 않도록 개인정보처리시스템, **개인정보 취급자의 컴퓨터**와 모바일기기에 조치	개인정보 취급자의 컴퓨터 (추가) 관리용 단말기, 업무용 컴퓨터 (삭제)	Endpoint DLP Network DLP
	망분리	⑦ 개인정보 저장관리되는 이용자수가 일일평균100만명이상이거나 정보통신서비스 매출액 100억원 이상인 경우 개인정보취급자의 컴퓨터 등에 외부인터넷망 차단조치	-	4조 접근통제 ⑥ 물리적 또는 논리적으로 망분리	망법고시 4조 ⑥항 망분리 조항이 개보법고시 6조 접근통제 ⑦로 이동	망분리 솔루션 망연계 솔루션
7조 개인정보의 암호화	암호화저장 개인정보	① 다음 개인정보는 안전한 암호 알고리즘으로 암호화하여 저장. 단, 비밀번호를 저장하는 경우에는 복호화 되지 아니하도록 일방향 암호화하여 저장. 1. 주민등록번호 2. 여권번호 3. 운전면허번호 4. 외국인등록번호 5. 신용카드번호 6. 계좌번호 7. 바이오인식정보 8. 비밀번호	7조 ①항 암호화 보관 대상 고유식별정보(주민, 여권, 운전면허, 외국인등록), 바이오정보, 비밀번호	6조 ②항 고유식별정보(주민, 여권, 운전면허, 외국인등록), 바이오정보, 비밀번호 **+ 신용카드번호, 계좌번호**	망법고시에 명시된 계좌번호, 카드번호까지 포함하여 암호화	Endpoint DLP Server DLP
	내부망 암호화	② 개인정보 및 인증정보를 정보통신망을 통하여 송·수신하는 경우 암호화 ③ 개인정보를 업무용 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장시 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장	7조 ④항 고유식별정보는 내부망 저장시 1. 영향평가 결과에 따라 2. 위험도분석에 따라 적용 나머지는 내부망 선택적용	6조 내부망, DMZ 상관없이 암호화	내부망과 DMZ 저장규정 삭제 DMZ 상관없이, 분리없이 암호화	
	DMZ 암호화		7조 ③항 고유식별정보는 DMZ 저장시 암호화			Server DLP
8조 접속기록의 보관 및 점검	접속기록보관	① 개인정보처리시스템 접속한 기록은 1년 이상 보관·관리. 단, 아래에 해당될 경우 접속기록을 2년 이상 보관관리 1. 「전기통신사업법」제5조의 규정에 따른 기간통신사업자 2. 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 자	8조 ①항 5만명 이상 개인정보 처리 또는 고유식별/민감정보 처리시 2년 이상 접속기록 보관	5조 접속기록 기본 1년 이상 보관 기간통신사업자는 2년이상 접속기록 보관	망법고시 5조 기간통신사업자 규정이 개보법고시 8조 ①항으로 이동	DB DLP 개인정보 접속기록관리
	조회된 개인정보주체	② 개인정보처리자는 개인정보 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 상 점검. 개인정보 다운로드한 것이 발견되었을 경우 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인	개인정보 다운로드 발견 내용으로 개인정보주체 파악	--	변동없음 개인정보보호법고시규정 유지	
	개인정보 다운로드 사유기록		기존 명시			
9조 악성코드	악성코드	악성프로그램을 방지 치료할 수 있는 백신 소프트웨어 등의 보안프로그램 설치운영	기존 명시	기존 명시		Endpoint DLP/EDR 안티바이러스
10조 관리용 단말기의 안전조치	관리용 단말기	관리용 단말기에 개인정보 유출 등 침해사고 방지를 위해 다음 조치 수행 1. 미인가 접속자 차단 2. 본래 목적외로 사용되지 않도록 조치 3. 악성프로그램 감염방지 조치 **4. 그 밖에 개인정보가 열람권한 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 조치**	1~3호만 기존명시	-	**10조 4호 신설** **4. 그 밖에 개인정보가 열람권한 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 조치**	Endpint DLP DB DLP
11조 물리적 안전조치	물리조치	① 전산실, 자료보관실 등 개인정보 보관 장소를 별도로 두고 있는 경우 출입통제절차 수립 및 운영 ② 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관 ③ 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 마련	기존 명시	기존 명시	개보법고시 11조 ③항 일부 조항 삭제 별도의 개인정보처리시스템을 운영하지 않고 업무용 컴퓨터, 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우 보조저장매체 반출입 통제대책 적용하지 아니할 수 있다	물리적 보호조치

조항	키워드	개정고시	기존 개보법고시	기존 망법고시	차이점	기술적 보호조치
12조 재해재난 대비 안전조치	백업	① 재해재난시 개인정보처리시스템 보호를 위한 대응매뉴얼 마련 ② 백업 및 복구계획 수립	기존 명시	-	변동없음 개인정보보호법 고시규정 유지	재해복구 절차 컨설팅
13조 출력복사시 안전조치	출력물	① 출력(인쇄, 표시, 생성) 용도 특정 및 출력항목 최소화	-	9조 ①항 출력복사시 안전조치	망법고시 9조 개보법고시 13조로 이동	개인정보 접속기록관리
		② 종이인쇄물, 개인정보파일이 포함된 외부저장매체 관리조치 구축	11조 물리적 안전조치에 서류 언급 (전산실, 자료보관실 통제절차)	9조 ②항 출력복사시 안전조치		Endpint DLP DB DLP
14조 개인정보 표시제한 안전조치	마스킹	개인정보 조회, 출력업무 수행시 개인정보 마스킹하여 표시제한	-	10조 개인정보 표시제한조치	망법고시 14조 개보법고시 14조로 이동	SI개발, 개인정보 접속기록관리
15조 개인정보의 파기	파기	개인정보를 파기할 경우 **현재 기술수준에서 사회통념상 적정한 비용**으로 개인정보 복원이 불가능하도록 조치	소각, 파쇄, 소자장비, 덮어쓰기, 천공, 마스킹 명시	-	파기방법은 **스스로 필요한 방법으로 처리할 수 있도록**으로 개정	Endpoint DLP Server DLP

(주)소만사 서울특별시 영등포구 영신로220 knk디지털타워 9층
Tel: 02 2636 8300 | Fax: 02 2636 8181 | Email: privacy@somansa.com