

중소기업 focus

중소기업이 알아야 할 정보보호법(1)

- 기업·기관의 주민등록번호 수집 제한 및 정보보호 주의의무 강화 -

발간주제

25호 : 기업·기관의 주민등록번호 수집 제한 및 정보보호 주의의무 강화

26호 : 정보유출 처벌 강화 및 정보유출 예방을 위한 중소기업 지원사업

하나. 주민등록번호 수집 제한

■ 주민등록번호 수집 최소화

* 법령에 근거가 없으면 주민등록번호 수집 불가(「개인정보 보호법」 제24조의2 - 주민등록번호 수집법정주의)

☞ 2014. 8. 7. 부터 법령에서 구체적으로 주민등록번호의 처리를 허용한 경우* 또는 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되거나 이에 준하는 경우 이외에는 주민등록번호 수집 불가

2014. 8. 7. 시행 「개인정보 보호법」
제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.
1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부(現행정자치부)령으로 정하는 경우
② 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

※ 주민등록번호 수집이 가능한 경우 사례(행정자치부, 2015. 2. 6.)

구 분	수집 가능 사례	법령상 근거
금융거래 상대방 신용도 조회	신용거래, 보증, 융자 등 거래 상대방의 신용도 조회를 위한 주민번호 수집	신용정보보호법
금융거래 시 실명 확인	은행 계좌 개설이나 적금상품 등 가입을 위한 주민번호 수집	금융거래실명거래 및 비밀보장에 관한 법률
휴대폰, 유선전화 등 통신서비스 가입	통신서비스 가입자 관리, 요금수납, 본인확인 업무수행 등을 위한 주민번호 수집	전기통신사업법, 정보통신망법
회사 직원 인사관리 및 급여 지급	회사 내 직원(정규직, 계약직 등)의 인사관리 및 급여지급을 위한 주민번호 수집	근로기준법, 고용보험법 등
기부금 영수증 발급	기부금품 모집이나 출연 받은 경우 기부금 영수증 또는 명세서 발급을 위한 해당 후원자의 주민번호 수집	소득세법, 상속세 및 증여세법 등
취약계층 대상 요금 감면	수도, 통신, 난방 요금 등 취약계층 대상 요금 감면을 위해 감면조건에 해당하는지 여부 확인을 위한 주민번호 수집	전기통신사업법, 수도법, 집단에너지사업법 등
부동산 계약 시	부동산 계약 시 확정일자 신고, 부동산 거래 신고 등을 위한 주민번호 수집	부동산 거래신고에 관한 법률 등
병·의원의 진료행위 및 약 처방	병원 진료, 진단서 발급 또는 처방전을 받아 약을 조제하는 경우 주민번호 수집	의료법 시행규칙

* 위반시 최고 3천만원 과태료 부과(「개인정보 보호법」 제75조 제2항 4의2)

☞ 한시적으로 도입했던 주민등록번호 수집법정주의 **계도기간('14.8.7.~'15.2.6.) 종료**

☞ 정부, 온·오프라인에서 이루어지는 주민등록번호 수집·처리에 대한 단속 대폭 강화 및 불법 주민번호 수집에 대한 엄정 처분 계획 발표('15.2.6.)

※ 주민등록번호 수집이 불가능한 경우 사례 (행정자치부, 2015. 2. 6.)

개인정보를 수집하고
처리하는 기업 담당자는
개인정보 업무 처리시 더욱
높은 주의 필요

구분	수집 불가능 및 전환 사례
멤버십 회원 가입	▶ 제휴사와 구매실적 공유 및 포인트 관리, 회원카드 미소지자 본인확인 등을 위한 주민번호 수집 불가능 ▶ 회원번호, 전화번호, 성명+생년월일 등으로 대체
입사지원 등 채용 관리	▶ 신입사원 채용시험 응시자 관리를 위한 주민번호 수집 불가능 ▶ 생년월일, 전화번호 등으로 대체
요금 자동이체 신청	▶ 매월 요금이 정산되는 계약 체결 시(신문, 할부 등) 금융기관 자동이체 신청을 위한 계약자의 주민번호 수집 불가능
대법원 판결서	▶ 민사·행정·특허 판결서에 주민번호를 기재하지 않기로 함
공정거래 표준약관	▶ 표준약관 개정을 통해 이사화물, 대부거래, 상조서비스, 국제결혼중개, 전자상거래(온라인 판매), 입원 약정서 등의 약관에 주민번호 기재란 삭제

■ 주민등록번호 수집 대체수단 도입

- * 적법하게 주민등록번호를 수집한 경우에도 반드시 암호화 조치를 통해 안전하게 관리해야 함
↳ 암호화는 '16. 1. 1. 부터 단계적 의무화
- * 각종 회원가입이나 계약 체결시 등에 있어서 주민등록번호 대신 본인확인 수단으로 활용될 수 있는 마이핀(My-PIN, 내번호) 서비스 도입·시행
↳ 13자리 무작위 번호로 구성, 홈페이지(www.g-pin.go.kr 등)나 동 주민센터에서 쉽게 발급

2

둘. 정보보호 주의의무 강화

※ 2014년 11월 29일 시행
「정보통신망 이용촉진 및
정보보호 등에 관한 법률」

■ 개정 정보통신망법* 주요 내용

변경 또는 신설 조항	미이행시 제재	비고
개인정보유출 사실을 안 때 24시간 이내에 이용자에게 통지하고, 방송통신위원회 또는 한국인터넷진흥원에 신고해야 함(제27조의3)	3천만원 이하의 과태료	24시간 경과의 정당한 사유를 소명하면 과태료 미부과
개인정보 파기시 복구·재생활 수 없도록 해야 함(제29조 제1항)	2년 이하의 징역 또는 2천만원 이하의 벌금	정보보호인력에 부과될 수 있는 벌칙조항 추가
개인정보가 유출된 경우 이용자는 300만원 이하의 법정 손해배상 청구 가능(제32조의2)	1인당 300만원 이하의 손해배상	법원 판결에 의함
일정 기준에 해당하는 사업자는 정보보호 최고책임자 지정(제45조의3)	3천만원 이하의 과태료	시행령에서 기준을 정함. 검임 가능
영리목적의 광고성 정보를 전송할 목적으로 전화번호를 자동으로 등록하는 조치, 수신자를 기망하여 회신을 유도하는 각종 조치 금지(제50조 제5항)	1년 이하의 징역 또는 1천만원 이하의 벌금	광고성 정보 수신자의 사전동의 필수
개인정보의 취급위탁시 위탁자가 관리·감독을 소홀히 하여 수탁자가 동법 제4장(개인정보의 보호)의 규정을 위반한 경우 과징금 부과(제64조의3 과징금 제1항 5의 2호)	위반행위 매출액의 3/100 이하 과징금	수탁자와의 계약과 점검 등 관리·감독 방법 검토 필요
개인정보가 유출된 경우로서 개인정보 보호조치(동법 제28조 제1항 2~5호)가 미비한 경우 과징금 부과(제64조의3 과징금 제1항 6호)	위반행위 매출액의 3/100 이하 과징금	개인정보 보호조치 관련 조항, 시행령, 시행규칙, 고시 엄수

*** 개인정보 유출을 안 경우 24시간 이내에 통지 및 신고 의무화**

☞ 24시간은 짧은 시간이므로, 개인정보 유출 시 고객 등 이용자들에게 통지할 내용과 규제기관에 신고할 내용, 신고 방법을 사전에 훈련하고 대비해둘 필요가 있음

기업의 정보보호책임자는
관련 개정 법률안을
확인하고,
대비체제를 점검하여
정보유출 피해를 차단할 수
있도록 사전 준비가 필요함

개인정보 유출 시 통지·신고 의무
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3(개인정보 누출등의 통지·신고) ① 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 "누출등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. 1. 누출등이 된 개인정보 항목 2. 누출등이 발생한 시점 3. 이용자가 취할 수 있는 조치 4. 정보통신서비스 제공자등의 대응 조치 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 ② 제1항의 신고를 받은 한국인터넷진흥원은 지체 없이 그 사실을 방송통신위원회에 알려야 한다. ③ 정보통신서비스 제공자등은 제1항 본문 및 단서에 따른 정당한 사유를 방송통신위원회에 소명하여야 한다. ④ 제1항에 따른 통지 및 신고의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다. ⑤ 정보통신서비스 제공자등은 개인정보의 누출등에 대한 대책을 마련하고 그 피해를 최소화할 수 있는 조치를 강구하여야 한다.

개인정보 유출 시 통지·신고 방법
「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제14조의2(개인정보 누출등의 통지·신고) ① 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 "누출등"이라 한다)의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다. ② 정보통신서비스 제공자등은 제1항에 따른 통지·신고를 하려는 경우 법 제27조의3제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 아니하였으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다. ③ 정보통신서비스 제공자등은 법 제27조의3제1항 각 호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제27조의3제1항 각 호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다. ④ 천재지변이나 그 밖의 정당한 사유로 제3항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고하는 것으로 제3항에 따른 홈페이지 게시를 갈음할 수 있다. ⑤ 정보통신서비스 제공자등은 법 제27조의3제1항 각 호 외의 부분 본문 및 단서에 따른 정당한 사유를 지체 없이 서면(전자문서를 포함한다)으로 방송통신위원회에 소명하여야 한다.

*** 개인정보를 파기할 때에는 복구·재생활 수 없도록 규정하고 위반시 처벌 강화**

☞ 개인정보를 파기할 때 복구·재생활 수 없도록 하려는 정보통신망법 제29조 1항의 문구는 개인정보보호법과 같지만, 개인정보보호법과는 달리 미이행시 2년 이하의 징역 또는 2천만원 이하의 벌금을 부과하는 벌칙조항이 신설됨(제73조 1의2호)

☞ 기존 개인정보 유출관련 벌칙조항 외에 기업의 인력이 형사처벌될 수 있는 조항이 하나 더 늘어난 것으로, 보유한 개인정보의 파기방법에 관해 심도있는 검토와 대비가 필요함

개인정보를 파기해야 하는 경우
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제29조(개인정보의 파기) ① 정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 해당 개인정보를 복구·재생활 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다. 1. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 수집·이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우 2. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용 기간이 끝난 경우 3. 제22조제2항에 따라 이용자의 동의를 받지 아니하고 수집·이용한 경우에는 제27조의2제2항제3호에 따른 개인정보의 보유 및 이용 기간이 끝난 경우 4. 사업을 폐업하는 경우

*** 정보보호 최고책임자 지정하지 않으면 과태료 부과**

☞ 일정 기준에 해당하는 사업자는 정보보호 최고책임자를 지정하고(제45조의3), 이를 신고하지 않으면 3천만원 이하의 과태료를 부과(제76조 제1항 6의2호)하도록 함으로써 정보보호 최고책임자 지정이 의무화됨

정보보호 최고책임자 지정 의무와 정보보호 최고책임자의 역할
<p>「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3(정보보호 최고책임자의 지정 등)</p> <p>① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정할 수 있다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하고 미래창조과학부장관에게 신고하여야 한다.</p> <p>② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.</p> <p>③ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.</p> <ol style="list-style-type: none"> 1. 정보보호관리체계의 수립 및 관리·운영 2. 정보보호 취약점 분석·평가 및 개선 3. 침해사건의 예방 및 대응 4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등 5. 정보보호 사전 보안성 검토 6. 중요 정보의 암호화 및 보안서버 적합성 검토 7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행 <p>④ 정보통신서비스 제공자는 침해사건에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있다.</p> <p>⑤ 정부는 제3항에 따른 정보보호 최고책임자 협의회에 필요한 경비의 전부 또는 일부를 지원할 수 있다.</p>
정보보호 최고책임자 지정·신고 대상 업체의 범위
<p>「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제36조의6(정보보호 최고책임자 지정·신고 대상자의 범위) 법 제45조의3제1항 단서에서 "종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자"란 정보통신서비스 제공자로서 다음 각 호의 어느 하나에 해당하는 자를 말한다.</p> <ol style="list-style-type: none"> 1. 법 제41조제1항제1호에 따른 내용 선별 소프트웨어를 개발 및 보급하는 사업자 2. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자 3. 「저작권법」 제104조제1항에 따른 특수한 유형의 온라인서비스제공자로서 상시 종업원 수가 5명 이상이거나 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 1천명 이상인 자 4. 「전자상거래 등에서의 소비자보호에 관한 법률」 제2조제3호에 따른 통신판매업자(통신판매중개업자를 포함한다)로서 상시 종업원 수가 5명 이상인 자 5. 「게임산업진흥에 관한 법률」 제2조제7호에 따른 인터넷컴퓨터게임시설제공업을 영위하는 자에게 같은 법 제28조제6호에 따라 고시된 음란물 및 사행성게임물 차단 프로그램을 제공하는 사업자 6. 상시 종업원 수가 1천명 이상인 자

■ 기업이 반드시 알아야 할 개인정보보호 수칙

- 하나. 적법한 방법으로 서비스 제공을 위한 최소한 개인정보를 수집하라.
- 둘. 개인정보를 제3자에게 제공하는 경우 반드시 이용자의 동의를 얻어라.
- 셋. 개인정보취급업무를 제3자에게 위탁하는 경우, 수탁업체에 대한 관리 감독을 철저히 하라.
- 넷. 개인정보 A~Z까지 책임질 수 있는 개인정보보호 관리책임자를 지정하라.
- 다섯. 고객의 개인정보를 어떻게 취급하는지에 대해 투명하게 밝혀라.
- 여섯. 수집된 개인정보를 안전하게 보관하라.
- 일곱. 개인정보취급자에 대한 개인정보보호 인식제고에 노력하라.
- 여덟. 개인정보보호 실태에 대한 정기적인 감사를 실시하라.
- 아홉. 개인정보 이용·제공과 관련된 정보주체의 권리 요구에 신속히 대처하라.
- 열. 개인정보의 이용 및 보유 목적이 달성된 경우에는 지체 없이 파기하라.

- 행정자치부, 『민간기업 개인정보보호 매뉴얼』

발행 경기중소기업종합지원센터
 발행인 윤 종 일
 주소 경기도 수원시 영통구
 광고로 107
 홈페이지 www.gsbc.or.kr
 자료문의 정책조사실
 031-259-7362

「중소기업 포커스」는 경기도 중소기업에게 제공하는 정보 자료로, 본지에 게재된 내용은 경기중소기업종합지원센터의 공식견해와 다를 수 있습니다.

◆ 본 자료는 경기중소기업종합지원센터 홈페이지 센터소식(발간책자)에서 보실 수 있습니다.