

기업 등 민간부문의 개인정보보호 대응책

신 각 철 (법제처 법제연구관)

최근 「개인정보」의 불법유출 사건을 계기로 정보사회 역기능에 대한 우려의 소리가 높아지고 있다.

이에 이번호에는 민간기업등에서 마련해야할 개인정보보호를 위한 종합대책의 기준을 제시한다. -편집자주-

「신용사회」의 기반 위축

최근에 「개인정보」 불법유출사건으로, 각 언론 기관에서는 「못믿을 신용사회」라고 지적하고 개인 신상정보의 불법유출, 거래 등에 관하여 심각한 우려를 제기하고 있다(동아일보 94. 9. 23, 중앙·조선·한국 등).

지난 6월에 공무원등이 292만건의 개인정보유출사건 이후, 9월 22일경 「지존파」 살인집단이 백화점과 신용카드회사의 것으로 보이는 「우수고객 회원명단」(1,200여명)을 입수하고 범행을 모의한 사건이 밝혀졌기 때문이다.

앞으로 컴퓨터시스템의 보급·확대로 기업등에서 개인정보처리가 더욱 늘어갈 전망이며, 이에 따라 불법유출·부정이용 등으로 인하여 국민의 기본권인 사생활의 비밀이 침해됨은 물론 범죄에

악용되어 생명·재산에까지 위협을 느끼고, 결과적으로 신용사회의 기반마저 무너뜨려 경제활동도 위축될 우려가 있다.

개인정보 보호조치는 민간부문도 해당

개인정보보호에 관한 종합적인 보안대책의 수립은 공공기관에 한하여만 실시되는 것이 아니라, 컴퓨터로 개인정보를 취급하는 경우는 모든 사업자가 법령에서 요구하는 보호조치를 강구할 의무가 있다.

특히 정보통신서비스업 예컨대, PC통신사업자, DB사업자 그 밖에 공공기관들로부터 용역을 위탁받아 정보처리를 하는 사업자등은 앞으로 개인정보보호에 관하여 특별한 대책을 마련해야 할 것이다.

더구나 95년 1월부터 우리나라에서 최초로 「개인정보보호법」(공공기관의 개인정보보호에 관한 법률)이 시행되고, 이 법률이 원칙적으로는 국가 행정기관·지방자치단체·기타 공공기관 등이 적용되지만, 공공기관으로부터 개인정보를 위탁받아 처리하는 기관·단체·기업 등도 이 법률의 적용을 받게 된다.

그러나 공공기관 이외의 개인 또는 단체 등 민간부문에서도 컴퓨터를 사용하여 개인정보를 처리함에 있어서 공공기관의 예에 준하여 개인정보 보호를 위한 필요한 조치를 강구하여야 한다는 규정(법 제22조)이 있다. 민간기업등에서도 개인정보보호를 위한 종합대책을 반드시 마련하여야 하겠기에 이에 대한 기준을 제시해 보고자 한다.

「개인정보보호 관리규정」의 기본적 사항

앞에서 밝힌 바와 같이 개인, 기업 등 민간부문에서도 개인정보보호법의 시행에 대비하여 개인정보보호관리규정을 제정하여 적절한 보호대책을 강구하도록 법률에서 명문화하고 있다.

특히, 최근에 문제가 되고 있는 백화점이나 기타 유통업계 등 민간부문에서도 개인정보를 고객 관리용으로 많은 인원(시행령에서 1,000명 이상)을 대상으로 컴퓨터처리하여 관리할 경우는 「개인정보보호관리규정」을 사내규정(社內規程)으로 제정·시행하여야 할 것이다.

이와같은 사내규정의 제정기준을 설정하는데 참고가 되도록 「개인정보보호법」과 OECD의 「프라이버시보호와 개인정보의 국제유통에 관한 지침」을 토대로 다음과 같이 반드시 규정에 포함되어야 할 6개의 원칙을 소개하고자 한다.

수집제한의 원칙

예를 들면 PC통신가입계약에 있어서 가입자의

① 정보통신서비스업을 영위하는 자가 서비스를 제공하기 위하여 수집하는 개인정보는 그 서비스 제공에 있어서 필요한 한도내에서만 수집해야 한다.

주소·성명·단말기기의 종류 및 설치장소, 요금 등 청구서 송부장소 등 서비스 제공에 반드시 필요한 정보만을 수집해야 한다. 또한 백화점등 유통부문에서도 판매관련 꼭 필요한 정보만을 수집해야 한다.

또한 개인의 사상·신조 기타 범죄경력 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보는 수집해서는 아니된다.

이 규정은 개인정보보호법 제4조에 명문으로 규정되었기 때문에 반드시 지켜야 한다. 기본적 인권이 침해될 우려가 있는 정보는 거래상 신용정보도 들 수 있다. 예컨대, 과산선고, 부도, 재산상태, 월수입 정도 등이 그 예에 해당된다.

수집하고자 하는 개인정보는 단말기설치에 필요한 정보(전화번호), 정보서비스제공상 필요정보(단말기 기종) 등 구체적으로 정보서비스 목적 달성을 필요한 정보만을 수집해야 한다.

개인정보의 수집은 원칙적으로 정보주체로부터 직접 수집해야 한다. 부득이 제3자로 부터 수집할 경우에는 정보주체의 이익을 부당하게 침해하지 아니하도록 유의하고 필요하다면 추후에 정보주체에게 수집내용을 통보하도록 한다.

개인정보의 비밀수집을 금지하기 위하여 개인정보보호법에는 그 수집목적·수집내용 등을 연1회 이상 관보에 게재하여 공고하도록 규정하고 있다(법 제7조 참조).

공공기관에서 관보등을 통하여 공고하는 취지는 직접 우편 등으로 정보주체에게 알릴 수 없기 때문에 일괄적으로 널리 알리기 위한 것이며, 「비밀수집」을 금지하기 위한 보장책이라고 보겠다.

목적 명확화의 원칙

개인정보의 수집은 수집목적을 명확히 하고 정보주체에게 알려야 하며, 적법하고 공정한 방법으로 수집하여야 한다.

이 목적명확화의 원칙은 수집제한·이용제한의 원칙과 밀접한 관련이 있다. 예컨대 단말기 기종, 전화번호 등의 정보수집 목적은 통신설비설치등에 필요하다. 따라서 직접 사업목적 달성과 관련 없는 정보의 수집은 이 원칙에 어긋난다고 볼 수 있다.

이용·제공제한의 원칙

① 개인정보의 이용은 원칙적으로 수집목적의 달성을 위한 범위안에서 이용하여야 한다. 다만 정보주체의 동의를 받았을 때에는 목적 이외로 이용할 수도 있다.

예컨대, 정보통신서비스의 제공을 위하여 수집된 개인정보는 통신회선의 설치, 설비의 보수관리, 요금의 청구와 기타 서비스 제공에 필요한 한도에서만 이용하여야 한다.

이와같은 한도를 초과하여 정보통신기기 판매 등 홍보우편물로 이용하는 것은 직접 수집한 회사라 하여도 목적외 사용이 된다.

② 수집목적 이외로 개인정보를 외부 제3자에게 이용·제공할 수 있는 경우는 다음 사항에 한한다. 그러나 정보주체의 권리와 이익을 부당하게 침해할 우려가 있다고 인정될 경우에는 그러하지 아니하다.

⑦ 정보가 주체의 동의가 있을 경우에는 외부에 제공할 수 있다.

④ 정보주체 이외의 자(제3자)에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정하

는 경우는 외부에 제공할 수 있다.

⑤ 특정개인 즉 정보주체를 식별할 수 없는 형태로 제공하는 경우는 개인의 권리가 침해되지 않기 때문에 제공이 가능하다.

⑥ 통계작성, 학술연구 기타 법령의 규정에 의하여 외부에 제공해야 하는 경우 또는 공공의 이익을 위하여 제공해야 할 상당한 이유가 있을 때에는 외부제공이 가능하다. 위의 4가지 요건 이외로 개인정보를 외부에 제공, 유통해서는 아니된다. 그밖에 정보통신설비의 보수관리 등을 외부사업자(AS업체)에게 위탁하였을 때에는 가입자의 주소·성명·단말기기종등 정보를 외부자(AS업체)에게 제공하되 비밀유지 의무가 부과되어야 한다.

③ 개인정보의 이용·제공은 개인정보보호법(제10조 : 이용·제공제한), 전기통신 사업법(제54조 : 통신의 비밀보호), 전산망보급확장과 이용촉진에 관한 법률(제25조 : 비밀보호)등 통신관계법률의 관련규정을 준수하여야 한다.

개인정보의 보호에 관해서는 헌법 제17조의 「사생활의 비밀과 자유의 보장」을 근거로 개인정보보호법, 전기통신사업법, 전산망법 등에 규정하고 있으며, 이에 대한 세부사항을 지켜야 한다.

안전성·정확성 확보의 원칙

① 개인정보를 처리함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성확보에 필요한 조치를 강구하여야 한다.

정보처리서비스업자 또는 기업 등은 개인정보를 취급함에 있어서 정보의 분실·도난·누출되지 않도록 시스템보안대책을 마련해야 한다. 사내규정(社內規程)으로 「전산자료안전관리규정」을 제정하여, 전산실의 통제, 책임자 지정, 중요

전산자료의 암호화 등 종합대책을 수립해야 한다. 즉 상당한 노력으로 「안전관리」를 해야 할 의무가 있다. 이를 계율리하여 개인정보가 누출되었을 때에는 관리책임자도 책임을 지게 된다.

② 개인정보가 정확하고 최신성을 확보하도록 노력하여야 한다.

잘못된 개인정보가 이용·제공될 경우 정보주체의 권리·이익이 침해된다. 예컨대 파산선고 또는 부도 등 전력(前歷)이 없음에도 잘못 처리되어 특정 개인의 경제활동에 막대한 피해를 줄 우려가 있다. 따라서 개인정보의 최신성·정확성을 유지해야 한다.

③ 개인정보는 원칙적으로 보존기간을 정해야 하고 보존기간을 초과한 정보는 지체없이 말소하도록 한다. 또한 이용목적을 달성하였을 경우에도 지체없이 말소한다.

예컨대, 정보처리서비스에 관한 요금청구 또는 유지보수와 관련된 개인정보를 수집하였을 경우, 요금이 회수되었거나 거래가 중단되어 필요없는 개인정보는 지체없이 말소해야 한다.

④ 개인정보를 외부에 위탁하여 처리하거나 또는 제3자에게 이용제공할 경우에는 위탁·사용계약에 있어서 반드시 비밀유지의무, 안전성확보의무를 명문화해야 한다.

예컨대, 공공기관으로부터 정보처리업자에게 개인정보(종합소득세)처리를 위탁하였고, 위탁받은 업자는 다른 업자에게 또한 하도급하는 경우가 있다. 이때 위탁계약 및 하도급계약에서 반드시 비밀유지의무·안전성확보의무를 명문화해야 한다.

개인참가의 원칙

① 정보주체는 자기의 개인정보에 관하여 열람을 청구할 권리가 있으며, 개인정보를 보유하고 있는 자는 이에 응하여야 한다.

예컨대, 정보처리서비스 업자가 고객의 개인정보를 보유·관리하고 있는 중에 정보주체로 부터 열람청구가 있을 경우 열람에 응해야 한다.

② 정보주체는 자기정보에 대하여 잘못 처리되었을 경우 정정 또는 삭제할 것을 청구할 수 있고 보유자는 지체없이 청구에 응해야 한다.

예컨대, 정보처리서비스업자가 고객의 개인정보하고, 열람결과 잘못 기록된 정보에 대하여 정정(訂正) 또는 말소를 요청하였을 때에는 보유자는 지체없이 이에 응해야 한다.

개인정보의 정확성·최신성을 확보하고 개인에 대한 「자기정보의 통제권」을 확보하기 위하여 「개인참가의 원칙」은 매우 중요한 원칙이다.

책임명확화의 원칙

개인정보를 취급함에 있어서 결정권한을 갖는 자는 개인정보보호법, 이 지침에 따라 개인정보보호에 관한 적절한 조치를 강구하고 내부체제의 정비 등을 도모하도록 노력해야 한다.

결정권한을 갖는 기업의 대표는 개인정보보호를 위하여 사내규정을 제정하고 이 규정에 따라서 보호조치를 강구하는 한편 지도·점검을 때때로 실시해야 한다. 또한 「시스템 감사체제」를 도입하여 내부적으로 정비하도록 하여야 한다.

개인정보처리등 시스템 보안대책

앞에서 제시한 6가지 원칙이 모두가 개인정보보호를 위한 중요한 원칙이지만 보다 강조하기 위

하여 시스템의 보안대책에 관하여 살펴보고자 한다.

시스템보안대책은 ① 기술적 보안 ② 물리적 보안 ③ 제도·법적 보안등으로 분류할 수 있다.

기술적보안대책은 컴퓨터 하드웨어, 소프트웨어, 정보 등에 대하여 비밀코드 부여 등 기술적인 방법을 들 수 있다.

물리적 보안대책으로는 전산시설의 접근금지, 별도의 특별관리시설 설치, 정보자료의 분산 등 시설관리 측면에서의 보안대책이다. 끝으로 법적·제도적 보안대책은 관리책임자지정, 업무의 분담, 시스템의 정기적 감사 등을 제도화하고 불법유출·부정이용자에 대하여 「형사법규에 의한 처벌강화」로서 범법행위를 예방하는 것을 의미한다.

이 글에서는 우선 공공기관이 적용받는 법적·제도적 보안대책을 간략히 소개하고, 민간부문에서도 공공기관의 예에 준하여 보안대책을 마련하도록 권장하고자 한다.

개인정보등 전산·정보 보안 법령

전산망법 제25조, 제30조에서 타인의 비밀정보 유출자에 대한 처벌규정이 있고, 개인정보보호법 제23조, 제24조에 벌칙규정이 있다(위 법률에서 부정이용자 처벌에 관해서는 「정보화사회」 94. 9 월호에 상세히 고찰한 바 있어 생략함). 따라서 이 글에서는 현재 시행되고 있는 훈령을 소개하고자 한다.

국무총리훈령(91. 5. 10 제250호)

「전산처리되는 개인정보보호를 위한 관리지침」

- 개인정보 무단유출방지대책

- 개인정보화일별 열람·입출력·전용단말기 지정

- 개인정보화일별 조작담당자 책임자 지정

- 개인정보 취급금지 조치

- 단말자별 개인코드, 비밀번호 및 단말기별 비밀장치 부여

- 특별한 경우 한하여 접근 허가, 화일 암호화

- 처리내역 일일보고체제 확립

- 개인정보처리내역 관리대장 작성

- 매일매일 관리책임자 확인 결재

- 무단유출·부정사용자 제재

- 무단유출·변조, 부정사용자 형벌외 징계

- 민간부문에 대한 행정적 제재 조치 강구

국가안전기획부 지침(지침 88.8)

「전산업무 보안관리지침」

- 전산실의 보안대책

- 외부로 부터 위해방지 출입문 통제

- 전산관리책임자 지정, 자료별 취급자지정

- 비밀자료 입력관리

- 정보파일별 비밀표시, 비밀장치 설정

- 비밀자료 출력관리

- 열람, 자료출력시 부서장의 승인

- 출력일시·면·장비의 고유번호 부착

- 열람·출력 등 책임자 확인·점검

총무처 지침

「행정전산망 안전관리지침」

- 단말기무단사용 방지

- 단말기 비밀번호 부여, 비인가자 취급금지

- 운용프로그램관리, 접근허가 카드 사용

- 출입자통제방안 강구 위한 관리책임자 지정

- 전산부서 직원 안전관리교육 강화 등

체신부 고시(93.2.2, 고시 제1993-6)

「전산망의 안전·신뢰성 기준」

- 전산망센터의 시설기준 설정

- 접근통제, 내부설비, 데이터 보관 등 기준 설정
- 전산망운용관리기준 설정
 - 세부안전·신뢰성 기준, 인사관리, 감리등
- 전산망 자원의 기술기준 설정
 - 데이터·소프트웨어관리, 접근통제, 컴퓨터바이러스 대책 등

기타 전산자원 안전관리 지침

내무부의 주민등록관리와 관련한 「전산자원안전관리지침」이 있으며 과학기술처·상공자원부 등 대부분의 중앙행정기관과 지방행정기관에서도 자체적으로 전산자원에 대한 안전관리지침을 제정하여 시행하고 있다.

이들 지침은 국가·지방자치단체, 정부투자기관, 교육기관 등 공공기관에서 의무적으로 지켜야 할 사항이며, 앞으로 민간부문도 이에 준하여 자체적으로 지침을 제정, 시행할 것을 관련기관에서 권고하게 될 것이다.

맺음말

앞으로 시행될 개인정보보호법 제22조 후단에서 「관계 중앙행정기관의 장은 개인정보의 보호를 위하여 필요한 때에는 공공기관외의 개인 또는 단체에 대하여 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다」라고 규정하였다.

예컨대, 정보처리서비스 업계에 대해서는 체신부장관이, 금융기관에 대해서는 재무부장관이, 기타 상공부문에 대해서는 상공자원부장관이 개인

정보보호에 관한 의견을 제시하고 보호조치를 강구하도록 권고하게 될 것이다.

우선적으로 정보처리서비스업자 등이 개인의 사생활비밀보호에 관한 인식과 이해를 보다 깊이 갖고 선도적으로 개인정보보호법의 취지에 따른 기본적 보호사항을 준수하도록 노력해야 할 것이다. 또한 관련단체·협회등에서도 자율적으로 「개인정보보호에 관한 지침」을 제정하여 홍보하고 권장할 필요가 있다.

최근의 언론보도에 의하면, 많은 국민들이 개인정보의 부정이용이 범행위인줄도 모르고 있으며 개인신상정보를 거래하는 판매조직이 전국에 걸쳐 성업중에 있다고 한다.

이러한 개인정보의 유출을 방지하기 위해서는 공공기관에만 법적 규제를 할 것이 아니라 민간부문도 규제하도록 강력한 입법조치와 함께 홍보교육이 시급하다고 한다.

그러나 앞에서 제시한 바와 같이 공공부문은 이미 제정된 「공 기관의 개인정보보호에 관한 법률」에 의하여 철저하게 관리하고, 민간부문은 우선 권장사항으로 자율적인 보호조치(社內規程等)를 강구하도록 해야할 것이다.

민간부문에 대한 지나친 법적 강제는 자유로운 경제활동을 위축시키고, 정보화추진에 역기능이 발생할 우려가 있기 때문에 바람직하지 않다는 관련 업계, 전문가의 의견에 따라 우선 공공기관부터 적용하도록 입법하였다.

그러나 앞으로 국민의 권리와 이익을 철저하게 보호하고 범죄예의 이용을 예방하기 위해 민간부문에 대한 규제조치도 마련되어야 할 것이다. ♦

**정보통신산업을 선도하는
한국정보통신진흥협회**