

제6장

전자상거래 정보의 보호

- 제 1 절 정보안전과 암호화방법
- 제 2 절 개인정보 보호 일반
- 제 3 절 전자상거래에 관한 정보의
보호

제 1 절 정보안전과 암호화방법

[I. 및 II. : 생략]

III. 전자서명

1. 전자서명의 의의와 효력

(1) 전자서명의 정의

전자서명은 일반문서의 서명과 같이 전자문서의 작성자와 내용의 진정을 증명할 수 있는 전자적 기법이다. 전자서명은 수기(手記) 서명에 대한 전자적 대안으로서, 수기 서명과 같은 또는 그 이상의 기능을 충족시킬 수 있다.

전자서명 모범법은 전자서명(electronic signature)을 “데이터메시지에 포함되거나, 첨부되거나 또는 논리적으로 결합된 전자적 형태의 데이터로서, 그 데이터메시지의 서명자를 확인하고 이에 포함된 정보에 대한 서명자의 승인을 표시하는데 사용될 수 있는 것”이라고 정의하고 있다^[2조]. 「전자서명법」은 모범법의 정의를 참고하여 전자서명을 “서명자의 신원 및 서명자가 해당 전자문서에 서명하였다는 사실을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보”라고 규정하고 있다^(전자서명법 2조).

전자서명은 공개키 암호화방법에 의한 디지털서명(digital signature)과 그 밖의 전자서명으로 나눌 수 있다. 현재 일반적으로 이용되고 있는 전자서명은 디지털서명이다. 종래 공인인증서에 기초한 공인전자서명이 인정되었으나, 이 제도는 2020년 6월 9일의 개정 「전자서명법」에 의하여 폐지되었다. 이것은 전자서명 기술의 발전에 따라 서비스 혁신을 고양하고 다양하고 편리한 전자서명수단^(전자서명법 2조)에 대해 국민들에게 선택권을 확대하기 위한 조치이다.⁹⁾

9) 국회 과학기술정보방송통신위원회, 전자서명법 전부개정법률안(대안), 의안번호 제24964호(2020. 5.) 참조.

(2) 디지털서명과 해쉬기능

1) 디지털서명 디지털서명이란 「디지털방식으로 암호화된 메시지에 수반되고 메시지의 발신인이 누구인지와 메시지가 발신인을 떠난 후에 변경되지 아니하였음을 증명할 수 있는 전자서명」을 말한다. 디지털서명은 공개키 암호화방법을 특정한 정보에 적용한 결과로서, 메시지의 발신인과 무결성을 확인하는데 사용하기 위하여 디지털방식으로 암호화된 데이터항목이다.

디지털서명의 원리는 다음과 같다. A가 그의 시스템에서 비밀키를 사용하여 전자서명을 생성한 후 평문에 서명을 하여 B에게 전송하고, B가 그의 시스템에서 A로부터 도착한 메시지에 A의 공개키를 사용하여 확인절차를 밟으면 그 메시지가 A로부터 전송되었다는 것과 그 메시지의 내용이 A의 시스템을 떠난 후에 변경되지 않았다는 것을 확인할 수 있다.¹⁰⁾ 디지털서명에서는 수신인이 발신인에 의하여 생성된 전자서명과 구별될 수 없는 디지털서명을 생성할 수 없다는 것을 전제로 한다. 디지털서명에서 메시지를 확인하는 키가 비밀리에 보관될 필요가 없다는 것은 곧 공개키방법을 사용하여 디지털서명이 설정될 수 있다는 것을 뜻한다.

2) 해쉬기능 전자서명은 메시지 내용의 전체에 대하여 암호화와 복호화가 적용되어야 하므로 전송되는 데이터의 분량은 적어도 원래의 메시지의 두 배가 된다. 이 문제를 개선하기 위하여 데이터 처리과정에 해쉬기능(hash function)이 도입된다. 해쉬기능이란 데이터 값을 커다란 영역으로부터 상대적으로 조그만 범위로 압축하여 모사(模寫)하는 기능을 말한다.¹¹⁾

해쉬기능은 서명될 메시지의 내용으로부터 메시지 다이제스트(message digest)라고 불리는 일정한 길이의 데이터항목을 생성하는 데 이용된다. 해쉬기능을 적용할 때 일반적으로 메시지에 대한 어떠한 변경도 별개의 다이제스트를 만들어낸다는 특성을 가진다. 메시지 다이제스트를 생성하기 위한 가장 유용한 해쉬기능은 해쉬 값으로부터 원문으로 되돌아갈 수 없는 일방적 해쉬기능(one-way hash function)으로 알려져 있다.¹²⁾

10) P. E. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape* 250(1997).

11) L. Loeb, *Secure Electronic Transaction* 44-45(1998).

12) See T. J. Smendinghoff, *supra* note 4, at 501.

RSA 방식에 의한 해쉬기능은 다음과 같다. 전송시스템은 해쉬기능을 적용하여 메시지 원본으로부터 다이제스트를 얻은 후, 여기에 암호화방법을 적용하여 메시지와 함께 전송될 서명을 부가한다. 수신시스템은 수신한 메시지에 해쉬기능을 적용하여 다이제스트를 다시 구성하고, 복호화기능을 적용하여 공개키로 서명을 해독한다. 여기에서 두 개의 다이제스트가 일치하면 수신인은 발신인이 비밀키를 소유하고 있다는 것과 메시지 내용이 전송 과정에서 변경되지 않았다는 것을 확인할 수 있다.¹³⁾

(3) 인증서

전자서명은 인증서(certificate)에 기초하여 행하여진다. 인증서란 “전자서명 생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보”를 말한다(^{2조 6호}). 여기에서 전자서명 생성정보란 “전자서명을 생성하기 위하여 이용하는 전자적 정보”를 말하는데(^{2조 3호}), 이것은 암호화 방법에서 말하는 비밀키(private key)를 뜻한다. 가입자란 “전자서명 생성정보에 대하여 전자서명인증사업자로부터 전자서명인증을 받은 자”를 말한다(^{2조 9호}). 인증서는 인증사업자의 비밀키를 사용하여 위조나 변조가 불가능한 실체적 데이터이다.

인증사업자는 인증서의 발급을 신청받은 후 신원증명이 된 자와 전자서명을 검증하기 위한 전자적 정보(이하 “전자서명검증정보”라 한다) 사이의 관련을 확인하면 인증서를 발급한다. 인증기관은 인증서의 진정성 및 무결성을 확보하기 위하여 그 인증서에 디지털서명을 부가한다. 가입자는 인증서의 정확성을 확인한 후 인증기관으로 하여금 공개하도록 지시하여 자신과 통신을 하려는 제3자가 이용할 수 있게 한다.

디지털서명의 경우 누구라도 인증사업자의 전자서명검증정보를 사용하여 인증기관의 디지털서명을 확인함으로써 인증서의 진정성 및 무결성을 확인할 수 있다.

(4) 전자서명의 효력

1) 전자서명의 효력에 관한 법규

(가) UNCITRAL 전자서명 모범법 전자서명 모범법은 전자서명의 효

13) R. Kalakota & A. B. Whinston, supra note 3, at 109, 110.

력에 관하여 다음과 같이 규정한다(6조).

① 법률이 특정인의 서명을 요구하는 경우 관련 합의를 포함한 모든 사정에 비추어 데이터메시지가 생성되거나 교신된 목적을 위하여 적절하도록 신뢰성 있는 전자서명이 사용된 때에는 데이터 메시지와 관련하여 그 요건이 충족된 것으로 본다(6조1항).

② ①의 규정은 그 요건이 의무의 형식으로 되어 있는 법률이 서명의 부존재의 효과만을 규정하든 관계없이 적용한다(6조2항).

③ 전자서명은 다음의 경우에는 ①의 규정에 의한 요건의 충족에 관하여 신뢰성이 있는 것으로 본다(6조3항).

- ㉠ 서명생성 데이터가 사용된 관계에서 서명자에게만 결합되고 다른 자에게 결합되지 아니할 것.
- ㉡ 서명생성 데이터가 서명 당시에 서명자의 지배에 속하고 다른 자의 지배에 속하지 아니하였을 것.
- ㉢ 서명의 시점 이후에 행하여진 전자서명에 대한 변경이 검색될 수 있을 것.
- ㉣ 서명에 관한 법적 요건의 목적이 관련 정보에 관하여 무결성(integrity)의 보장을 제공하는 것일 경우에는 그 정보에 대하여 서명 시점 이후에 행하여진 변경이 검색될 수 있을 것.

④ ③의 규정은 다음의 권능을 제한하지 아니한다(6조4항).

- ㉠ 위의 ①에 규정된 요건을 충족하기 위하여 전자서명의 신뢰성을 다른 방법에 의하여 설정하는 것.
- ㉡ 전자서명의 비신뢰성의 증거를 제시하는 것.

(나) 유럽연합의 전자서명 지침 유럽연합의 「전자서명 지침」(1999)은 전자서명을 일반 전자서명과 고급 전자서명(advanced electronic signature)으로 구분하고, 적격 인증서에 기초한 고급전자서명은 전자적 형태인 데이터와 관련하여 수기 서명과 마찬가지로 서명의 법적 요건을 충족하며, 법적 절차에서 증거로서 허용될 수 있음을 명시하고 있다(5조1항). 여기에서 고급 전자서명이란 서명자에게 유일하게 속하고, 서명자를 확인할 수 있으며, 서명자가 그의 단독 관리 아래 유지하는 수단을 사용하여 생성하였고, 서명 후의 데이터 변경이 추적될 수 있는 방법으로 관련된 데이터

에 연결되어 있다는 요건을 충족하는 서명을 말한다⁽²³⁾. 이것은 우리나라의 공인전자서명에 준하는 전자서명을 가리킨다.

(다) 미국의 통일전자거래법과 연방 전자서명법 미국의 「통일전자거래법」(UETA)은 서명이 전자적 형태로 되어 있다는 이유만으로 법적 효력 또는 강제성이 부인되지 아니하며, 법률이 서명을 요구하는 경우 전자서명은 법률의 요건을 충족한다고 규정한다^{(7)(a)}. 전자서명의 귀속에 관하여는, 전자서명은 그것이 어떤 자의 행위인 경우에 그 자에게 귀속될 수 있고, 이러한 행위는 전자서명이 귀속될 수 있는 자를 결정하기 위하여 적용된 보안절차의 효과의 제시를 포함하여 어떠한 방식으로든 제시될 수 있다고 규정한다^{(9)(a)}. 이 규정에 의하여 어떤 자에게 귀속되는 전자기록 또는 전자서명의 효력은 당사자의 합의나 그 밖의 법률 규정을 포함하여 그 생성, 실행 또는 채택의 시점에서 전후관계와 주변상황에 의하여 판단한다^{(9)(b)}.

미국의 「연방 전자서명법」(ESIGN Act)¹⁴⁾은 주간통상과 국제통상에서 전자기록 및 전자서명의 사용을 원활하게 하여 전자계약의 법적 효력을 확보하기 위한 법률이다. 이 법은 전자서명의 유효성에 관하여 다음과 같이 규정하고 있다. 즉, 주간통상 또는 대외통상에 영향을 미치는 거래에 관하여, 그 거래에 관련된 서명, 계약 또는 기타의 기록은 전자적 형태로 되어 있다는 이유만으로 법적 효력, 유효성 또는 강제성이 부인되지 아니한다^{(10)(a)}. 해당 거래에 관련된 계약은 전자서명 또는 전자기록이 사용되었다는 이유만으로 법적 효력, 유효성 또는 강제성이 부인되지 아니한다^{(10)(b)}.

(라) 오스트레일리아 전자거래법 이 법은 연방의 법률에 따라 특정인의 서명이 요구되는 경우, 전자통신과 관련하여 특정인의 신원을 확인하고 송달된 정보에 관하여 특정인의 의사를 나타내는 방법 등이 사용되는 때, 관련 약정에 비추어 전자통신이 생성 또는 송달된 목적을 위하여 적합하도록 신뢰성이 있는 때 등에 있어 전자통신과 관련하여 해당 요건이 충족된 것으로 본다고 규정하고 있다⁽¹⁰⁾.

(마) 우리나라의 전자서명법 현행 「전자서명법」은 전자서명의 효력에 관하여 다음과 같이 규정하고 있다.

14) Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464(2000), 15 U.S.C. §7001 et seq.

① 전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 아니한다(전서 3조₁항).

② 법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다(전서 3조₂항).

전자서명의 효력에 관한 위의 규정은 서명요건의 충족과 전자서명의 증거력에 관한 것으로 전자서명 모범법(6조)과 궤를 같이하는 것이다.

2) 서명요건의 충족 법률은 중요한 계약에 관하여는 문서를 서면으로 작성할 것을 요구하고 또 계약상 구속력을 받을 자가 서명하거나 기명날인할 것을 요구하는 것이 보통이다. 이러한 경우 전자문서는 “서면으로 작성할 것” 및 “서명 또는 기명날인될 것”을 요구하는 법률의 요건을 충족시켜야 할 것이다.

앞에서 본 바와 같이, 전자서명 모범법은 법률이 특정인의 서명을 요구하는 경우 관련 합의를 포함한 모든 사정에 비추어 데이터메시지가 생성되거나 교신된 목적을 위하여 적절하도록 신뢰성 있는 전자서명이 사용된 때에는 데이터 메시지와 관련하여 그 요건이 충족된 것으로 보며(6조₁항), 이 규정은 그 요건이 의무의 형식으로 되어 있는 법률이 서명의 부존재의 효과만을 규정하든 관계없이 적용한다(6조₂항)고 규정하고 있다.

「전자서명법」은 서명요건의 충족을 명백히 하여 “법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다”고 규정하고 있다(전서 3조₂항).

3) 진정성 및 무결성의 추정

전자서명은 진정성(authenticity)과 무결성(integrity)이 추정될 수 있다. 앞에서 본 바와 같이, 전자서명 모범법은 전자서명이 일정한 요건[앞의 1] (가) 참조]을 갖춘 경우에는 서명요건에 관하여 신뢰성이 있는 것으로 본다(6조₃항).

(가) 진정성의 추정 진정성(authenticity)은 전자문서의 근원에 관한 것, 즉 수신한 전자문서가 누구로부터 전송되었으며 진정한 것인가의 문제이다. 전자서명이 있는 경우 그 전자서명이 서명자의 서명이라는 요건, 즉

진정성이 충족되어야 그 전자서명을 신뢰할 수 있을 것이다.

디지털서명의 경우 그 전자서명이 발신인의 전자서명검증정보를 사용하여 확인될 수 있으면 이에 대응하는 전자서명생성정보에 의하여 생성되었다는 것이 추정될 수 있다. 또 전자서명은 발신인이 전자문서의 근원으로서의 자기의 신원을 확인할 의도로 부가되었다는 것이 추정될 수 있다.

(나) 무결성의 추정 무결성(integrity)은 전자문서의 정확성 및 완전성에 관한 것, 즉 수신한 전자문서가 발신인이 전송한 전자문서와 동일한 것이고 완전한 것인가, 그리고 전송 중에 변경되지 않았는가의 문제이다. 무결성은 특히 전자상거래에서 온라인계약을 체결하거나 후에 그 거래를 증명하기 위하여 전자기록을 이용할 때 매우 중요하다.

「전자서명법」은 전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 아니한다고 규정하고 있다(전자서명법 제3조), 디지털서명의 경우 그 전자서명이 발신인의 전자서명검증정보에 의하여 확인될 수 있으면 그 전자문서는 전자서명이 생성된 후에 변경되지 않았다는 것이 추정될 수 있다.

4) 부인방지 부인방지(non-repudiation)란 발신인에게 전자문서를 귀속시키는 것, 즉 발신인이 그 전자문서의 전송을 부인하거나 수신된 전자문서가 전송한 내용과 동일하지 않다고 주장할 수 없다는 것을 말한다.

부인방지는 거래의 상대방에게 적용된다. 즉, 발신인을 구속함은 물론 수신인도 전자문서를 수신하였음을 부인하는 것이 배척된다. 부인방지는 전자문서를 신뢰한 당사자가 상대방에게 그 전자문서를 귀속시키려고 할 때 법적 요건이 된다.

5) 제3자의 신뢰권 전자문서상의 전자서명이 수신인에 의하여 확인될 수 있는 경우 수신인은 그 전자문서를 신뢰할 권리(right to rely)가 있고, 전자서명을 한 발신인은 그에 따른 구속력을 받게 될 것이다. 전자서명을 신뢰한 자는 인증서에 의하여 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 신뢰한 것으로 추정할 수 있다.

(5) 전자문서의 시점확인

전자서명인증사업자는 가입자 또는 이용자의 요청이 있는 경우 전자문서가 해당 전자서명인증사업자에게 제시된 시점을 전자서명하여 확인할 수

있다^(전자서명법 제18조).

시점확인(타임스탬핑)은 전자서명이 생성된 시기에 의하여 전자문서의 작성시기를 확정하는 확정일부(date/time stamping) 서비스를 응용한 것이다. 여기에서 일부란 전자문서, 전자서명 또는 인증서에 날짜, 시간과 사람의 신원을 나타내기 위하여 디지털서명된 기수법(記數法, notation)을 말한다.

2. 전자서명에 관한 정책 및 지원

「전자서명법」은 전자서명에 대한 정부의 정책과 지원을 규정하고 있다.

(1) 전자서명의 발전을 위한 시책 수립

정부는 전자서명의 안전성, 신뢰성 및 전자서명수단의 다양성을 확보하고 그 이용을 활성화하는 등 전자서명의 발전을 위하여 다음의 사항에 대한 시책을 수립·시행한다^(전자서명법 제4조). 여기에서 전자서명수단이란 “전자서명을 하기 위하여 이용하는 전자적 수단”을 말한다^(전자서명법 제2조).

① 전자서명의 신뢰성 제고, 전자서명수단의 다양성 확보 및 전자서명의 이용 활성화.

② 전자서명 제도의 개선 및 관계 법령의 정비.

③ 가입자 및 이용자의 권익 보호.

④ 전자서명의 상호연동 촉진.

⑤ 전자서명 관련 기술개발, 표준화 및 인력 양성.

⑥ 전자서명의 신뢰성 확보를 위한 안전한 암호 사용.

⑦ 외국의 전자서명에 대한 상호인정 등 국제협력.

⑧ 공공서비스에서 사용하는 전자서명의 안전한 관리.

⑨ 그 밖에 전자서명의 발전을 위하여 필요한 사항.

(2) 전자서명의 이용 촉진을 위한 지원

과학기술정보통신부장관은 전자서명의 이용을 촉진하기 위하여 다음의 사항에 대한 행정적·재정적·기술적 지원을 할 수 있다^(전자서명법 제5조).

① 전자서명 관련 기술의 연구·개발·활용 및 표준화.

② 전자서명 관련 전문인력의 양성.

③ 다양한 전자서명수단의 이용 확산을 위한 시범사업 추진.

④ 전자서명의 상호연동 촉진을 위한 기술지원 및 연동설비 등의 운영.

- ⑤ 인정기관^(전서 9조) 및 평가기관^(전서 10조)의 업무 수행 및 운영.
- ⑥ 그 밖에 전자서명의 이용 촉진을 위하여 필요한 사항.

(3) 다양한 전자서명수단의 이용 활성화

국가는 생체인증, 블록체인 등 다양한 전자서명수단의 이용 활성화를 위하여 노력하여야 한다^(전서 6조 1항). 블록체인(blockchain)이란 “블록”을 잇따라 “연결”한 모음을 가리킨다(후술 “Ⅳ. 블록체인 기술” 참조).

국가는 법률, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙, 대통령령 또는 감사원규칙에서 전자서명수단을 특정한 경우를 제외하고는 특정한 전자서명수단만을 이용하도록 제한하여서는 아니 된다^(전서 6조 2항).

(4) 전자서명인증 정책의 지원 등

한국인터넷진흥원은 전자서명을 안전하고 신뢰성 있게 이용할 수 있는 환경을 조성하고 전자서명인증 정책을 지원하기 위하여 다음의 업무를 수행한다^(전서 21조).

- ① 전자서명인증 관련 기술개발·보급 및 표준화 연구.
- ② 전자서명인증 관련 제도 연구 및 상호인정 등 국제협력 지원.
- ③ 전자서명인증사업자에 대한 검사^(전서 16조 1항) 지원.
- ④ 그 밖에 전자서명인증 정책의 지원에 필요한 사항.

3. 인증사업자의 인증업무 운영과 책임

전자서명인증이란 “전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위”를 말하고^(전서 2조 5호), 전자서명인증업무란 “전자서명인증, 전자서명인증 관련 기록의 관리 등 전자서명인증서비스를 제공하는 업무”를 말한다^(전서 2조 7호). 전자서명인증사업자란 “전자서명인증업무를 하는 자”를 말한다^(전서 2조 8호).

아래에서는 전자서명인증사업자의 인증업무 운영과 책임에 대하여 살펴본다.

(1) 전자서명인증업무 운영기준

과학기술정보통신부장관은 전자서명의 신뢰성을 높이고 가입자 및 이용자가 합리적으로 전자서명인증서비스를 선택할 수 있도록 정보를 제공하기

위하여 필요한 조치를 마련하여야 한다(전서 7조_{1항}).

과학기술정보통신부장관은 다음의 사항이 포함된 전자서명인증업무 운영 기준(이하 “운영기준”이라 한다)을 정하여 고시한다. 이 경우 운영기준은 국제적으로 인정되는 기준 등을 고려하여 정하여야 한다(전서 7조_{2항}).

- ① 전자서명 및 전자문서의 위조·변조 방지대책.
- ② 전자서명인증서비스의 가입·이용 절차 및 가입자 확인방법.
- ③ 전자서명인증업무의 휴지·폐지 절차.
- ④ 전자서명인증업무 관련 시설기준 및 자료의 보호방법.
- ⑤ 가입자 및 이용자의 권익 보호대책.
- ⑥ 그 밖에 전자서명인증업무의 운영·관리에 관한 사항.

(2) 운영기준 준수사실의 인정 등

1) 운영기준 준수사실의 인정 전자서명인증사업자(전자서명인증업무를 하려는 자를 포함한다)는 「전자서명법」 제9조에 따른 인정기관으로부터 운영기준의 준수사실에 대한 인정을 받을 수 있다. 이 경우 「전자서명법」 제10조에 따른 평가기관으로부터 운영기준의 준수 여부에 대한 평가를 먼저 받아야 한다(전서 8조_{1항}). 이 규정 전단에 따른 인정(이하 “운영기준 준수사실의 인정”이라 한다)을 받으려는 전자서명인증사업자는 국가기관, 지방자치단체 또는 법인이어야 한다(전서 8조_{2항}).

임원 중에 다음의 어느 하나에 해당하는 사람이 있는 법인은 운영기준 준수사실의 인정을 받을 수 없다(전서 8조_{3항}).

- ① 피성년후견인.
- ② 파산선고를 받고 복권되지 아니한 사람.
- ③ 금고 이상의 실형을 선고받고 그 집행이 끝나거나(끝난 것으로 보는 경우를 포함한다) 면제된 날부터 2년이 지나지 아니한 사람.
- ④ 금고 이상의 형의 집행유예를 선고받고 그 유예기간 중에 있는 사람.
- ⑤ 법원의 판결 또는 다른 법률에 따라 자격이 상실되거나 정지된 사람.

운영기준 준수사실의 인정을 받은 전자서명인증사업자는 과학기술정보통신부령으로 정하는 바에 따라 운영기준을 준수한다는 사실을 표시할 수 있다(전서 13조_{1항}). 운영기준 준수사실의 인정을 받지 아니한 자(유효기간 도과 등의 사유로 운영기준 준수사실의 인정의 효력이 상실된 자를 포함한다)는 이 규정

에 따른 표시 또는 이와 유사한 표시를 하여서는 아니 된다(전서 13조²항).

2) 인정기관 과학기술정보통신부장관은 「정보통신법」 제52조에 따른 한국인터넷진흥원(이하 “한국인터넷진흥원”이라 한다)을 운영기준 준수사실의 인정에 관한 업무를 수행하는 기관(이하 “인정기관”이라 한다)으로 지정할 수 있다(전서 9조¹항).

인정기관은 평가 결과를 제출받은 경우(전서 10조³항) 그 평가 결과와 운영기준 준수사실의 인정을 받으려는 전자서명인증사업자가 운영기준 준수사실의 인정(전서 8조)에 따른 자격을 갖추었는지 여부를 확인하여 운영기준 준수사실의 인정 여부를 결정하여야 한다(전서 9조²항). 인정기관은 해당 전자서명인증사업자에게 이 업무를 수행하는 데 필요한 비용을 징수할 수 있다(전서 9조⁴항).

인정기관은 위의 규정에 따라 운영기준 준수사실을 인정하는 경우 그 인정내용 및 유효기간이 기재된 증명서를 해당 전자서명인증사업자에게 발급하여야 한다. 이 경우 대통령령으로 정하는 바에 따라 증명서 발급사실을 공고하여야 한다(전서 9조³항). 인정기관은 해당 전자서명인증사업자에게 이 업무를 수행하는 데 필요한 비용을 징수할 수 있다(전서 9조⁴항).

운영기준 준수사실의 인정 여부 결정 및 인정 취소 등 업무수행방법, 운영기준 준수사실의 인정의 유효기간, 그 밖에 필요한 사항은 대통령령으로 정한다(전서 9조⁵항).

3) 평가기관 과학기술정보통신부장관은 전자서명에 관한 평가 업무(전서 8조¹항 후단)를 수행하는 기관(이하 “평가기관”이라 한다)을 선정하여 고시할 수 있다(전서 10조¹항).

운영기준 준수사실의 인정을 받으려는 전자서명인증사업자는 평가기관에 평가를 신청하여야 한다(전서 10조²항). 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대한 평가를 하고, 그 결과를 인정기관에 제출하여야 하며(전서 10조³항), 평가기관은 전자서명인증사업자에게 제3항의 업무를 수행하는 데 필요한 비용을 징수할 수 있다(전서 10조³항-4항).

평가기관의 선정기준·절차, 평가방법 등 업무수행방법, 운영기준 준수 여부에 대한 평가기준·절차, 그 밖에 필요한 사항은 대통령령으로 정한다(전서 10조⁵항).

과학기술정보통신부장관은 운영기준에 부합한다고 인정하는 국제적으로 통용되는 평가(“국제통용평가”)를 정하여 고시할 수 있다. 전자서명인증사업자가 국제통용평가를 받은 경우에는 평가기관의 평가를 받은 것으로 본다(전서 11조 1항·2항 전단).

과학기술정보통신부장관은 평가기관이 정당한 사유 없이 평가 업무를 하지 아니한 경우 등에 해당하는 경우에는 평가기관의 선정을 취소하거나 1년 이내의 기간을 정하여 해당 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 거짓이나 그 밖의 부정한 방법으로 평가기관으로 선정된 경우와 업무정지 기간 중에 평가 업무를 한 경우에는 그 선정을 취소하여야 한다(전서 12조 1항 12조). 이 규정에 따라 선정을 취소하려면 청문을 하여야 한다(전서 12조 2항).

4) 검사·시정명령 전자서명인증업무의 안전성과 신뢰성 확보 및 가입자의 보호 등을 위하여 과학기술정보통신부장관은 검사 및 시정명령의 권한을 가진다(전서 16조 17조).

(3) 전자서명인증업무준칙의 준수

운영기준 준수사실의 인정을 받은 전자서명인증사업자는 다음의 사항이 포함된 전자서명인증업무준칙(이하 “인증업무준칙”이라 한다)을 작성하여 인터넷 홈페이지 등에 게시하고 성실히 준수하여야 한다. 인증업무준칙을 변경한 경우에도 또한 같다(전서 15조 1항 15조).

- ① 전자서명인증서비스의 종류.
- ② 전자서명인증서비스의 요금, 이용범위 및 유효기간 등 이용조건.
- ③ 전자서명인증업무의 수행방법 및 절차.
- ④ 그 밖에 전자서명인증업무의 수행에 필요한 사항.

운영기준 준수사실의 인정을 받은 전자서명인증사업자는 전자서명인증업무의 전부 또는 일부를 휴지하려는 경우 휴지기간을 정하여 휴지하려는 날의 30일 전까지 그 사실을 가입자에게 통보하고 인터넷 홈페이지 등에 게시하여야 한다(전서 15조 2항 15조).

운영기준 준수사실의 인정을 받은 전자서명인증사업자는 전자서명인증무역을 폐지하려는 경우 폐지하려는 날의 60일 전까지 그 사실을 가입자에게 통보하고 인터넷 홈페이지 등에 게시하여야 한다(전서 15조 3항 15조).

위의 규정들에 따라 통보하거나 게시하는 내용에는 요금의 반환, 가입자

의 개인정보 폐기 등 가입자 보호조치가 포함되어야 한다^(전자서명법 제15조 제4항).

인증업무준칙의 작성방법, 위의 게시·통보 방법, 그 밖에 필요한 사항은 과학기술정보통신부령으로 정한다^(전자서명법 제15조 제5항).

(4) 전자서명인증사업자의 손해배상책임

운영기준 준수사실의 인정을 받은 전자서명인증사업자가 전자서명인증업무의 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상하여야 한다. 다만, 전자서명인증사업자가 고의 또는 과실이 없음을 입증하면 그 배상책임이 면제된다^(전자서명법 제20조 제1항).

운영기준 준수사실의 인정을 받은 전자서명인증사업자는 위의 규정에 따른 손해를 배상하기 위하여 대통령령으로 정하는 바에 따라 보험에 가입하여야 한다^(전자서명법 제20조 제2항).

4. 전자서명 관련 정보의 보호

「전자서명법」은 이용자의 정보보호를 위하여 전자서명생성정보의 보호와 인증서의 부정사용 방지를 위한 규정을 두고 있다.

1) 전자서명생성정보의 보호 누구든지 타인의 전자서명생성정보를 도용하거나 누설해서는 아니 된다^(전자서명법 제19조 제1항). 전자서명생성정보는 전자서명을 생성하기 위하여 이용하는 전자적 정보로서^(전자서명법 제2조 제3호 참조) 전자서명을 한 자의 신원을 확인할 수 있는 수단이 된다.

위의 규정을 위반한 자는 형사제재를 받는다^(전자서명법 제24조 제1항 1호).

2) 인증서의 부정사용 금지 누구든지 운영기준 준수사실의 인정을 받은 전자서명인증사업자가 발급하는 인증서와 관련하여 다음에 해당하는 행위를 하여서는 아니 된다^(전자서명법 제19조 제2항).

① 거짓이나 그 밖의 부정한 방법으로 타인의 명의로 인증서를 발급받거나 발급받을 수 있도록 하는 행위. 이와 같이 타인의 명의로 공인인증서를 발급받거나 발급받을 수 있도록 하면 전자서명의 부정사용이 가능해지기 때문이다^[판례]. 이 규정을 위반한 자는 형사제재를 받는다^(전자서명법 제24조 제1항 2호).

[판례 1] 타인명의로 공인인증서를 발급받는 행위

「전자서명법 제23조 제2항은 “누구든지 타인의 명의로 공인인증서를 발급 받거나 발급받을 수 있도록 하여서는 아니 된다”고 규정하고 있는 바, 위 조항의 입법 취지 및 조문체계, 전자서명법 제23조 제1항 내지 제5항에서 금지하고 있는 각 행위의 유형 및 그 위반에 대한 처벌의 정도 등에 비추어 보면, 위 조항에서 ‘타인의 명의로 공인인증서를 발급받거나 받을 수 있도록 하는 행위’라 함은 타인의 전자서명생성정보에 대한 지배·관리권을 배제하여 그 전자서명생성정보와 공인인증서 발급에 필요한 자료를 취득한 다음 그 타인의 명의로 공인인증서를 발급받는 행위 또는 이와 같이 공인인증서를 발급받을 수 있도록 하는 행위를 의미한다. 따라서 전자서명생성정보에 대한 지배·관리권을 계속하여 유지하고 있는 타인의 승낙 또는 위임을 받아 그 명의로 공인인증서를 발급받은 경우에는 전자서명법 제31조 제3호, 제23조 제2항을 적용하여 처벌할 수 없다.¹⁵⁾

② 부정하게 행사하게 할 목적으로 인증서를 타인에게 양도 또는 대여하거나, 부정하게 행사할 목적으로 인증서를 타인으로부터 양도 또는 대여받는 행위. 이 규정을 위반한 자는 형사제재를 받는다(전자서명법 제24조).

판례는 개정 전의 「전자서명법」에 따른 공인인증서에 관하여 “대여”라 함은 다른 사람으로 하여금 명의자의 관리·감독 없이 실질적으로 명의자와 마찬가지로 지위에서 그 공인인증서를 사용하여 그 명의자의 명의로 된 전자문서를 작성할 수 있도록 허용하는 것을 의미한다고 한다(판례).

[판례 2] 인증서의 대여

「전자서명법 제23조 제5항은 누구든지 행사하게 할 목적으로 다른 사람에게 공인인증서를 양도 또는 대여하거나 행사할 목적으로 다른 사람의 공인인증서를 양도 또는 대여받아서는 아니 된다고 규정하고 있는 바, 전자문서의 안전성과 신뢰성의 확보를 목적으로 하는 전자서명법의 입법 취지에 비추어 볼 때, 여기서의 ‘대여’라 함은 다른 사람으로 하여금 명의자의 관리·감독 없이 실질적으로 명의자와 마찬가지로 지위에서 그 공인인증서를 사용하여 그 명의자의 명의로 된 전자문서를 작성할 수 있도록 허용하는 것을 의미한다고 해석하여야 할 것이다.

피고인들이 공소외인으로 하여금 전혀 간섭받지 아니한 채 피고인들의 공인인증서를 사용하여 마음대로 피고인들 명의의 전자문서를 작성하도록 허용한

15) 대법원 2009. 5. 14. 선고 2008도11361 판결.

것은 앞서 본 법리에 비추어 공인인증서를 대여한 것으로 보아야 할 것이므로, 피고인들이 그들 명의의 공인인증서를 공소외인에게 대여한 다음 그 유효기간이 만료되자 이를 갱신하게 하였다면 그로써 이를 다시 대여한 것이라고 봄이 상당하다.»¹⁶⁾

3) 전자서명 관련 개인정보의 보호 등 전자서명 관련 정보는 개인정보에 속하므로 「개인정보 보호법」에 의하여 보호를 받는다.

또 전자서명은 정보통신망을 통하여 많이 사용되므로 「정보통신망법」이 규정하는 정보통신망에서의 권리보호에 관한 규정에 의하여 보호를 받는다.

IV. 블록체인 기술

1. 블록체인의 의미

국가는 생체인증, 블록체인 등 다양한 전자서명수단의 이용 활성화를 위하여 노력하여야 하고, 또 법률, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙, 대통령령 또는 감사원규칙에서 전자서명수단을 특정한 경우를 제외하고는 특정한 전자서명수단만을 이용하도록 제한하여서는 아니 된다^(천서 6조). 이 규정은 다양한 전자서명수단의 이용 활성화를 명시한 것이다.

블록체인(blockchain)이란 “블록(block)”을 잇따라 “연결(chain)”한 모음을 가리킨다. 비트코인 등의 암호화폐를 발행하고 관리하는 핵심 기법은 블록체인(blockchain) 기술인데, 각 암호화폐 코인의 유효성은 블록체인에 의하여 부여된다.

블록체인은 지속적으로 늘어나는 기록(블록)의 일람표로서 블록은 암호화방법을 사용하여 연결되어 보안이 확보된다. 각 블록은 전형적으로는 이전 블록의 암호해쉬, 타임스탬프와 거래 데이터를 포함한다. 고안에 의하여 블록체인은 처음부터 데이터의 수정에 대하여 저항력을 가지고 있다. 이것은 양당사자 간의 거래를 유효하게 영구적으로 증명할 수 있도록 기록할

16) 대법원 2008. 11. 27. 선고 2008도4963 판결.

수 있는 공개된 분산장부이다.¹⁷⁾ 분산장부로서의 이용을 위하여 하나의 블록은 새로운 블록을 유효하게 하기 위한 프로토콜에 집합적으로 부착하는 P2P 네트워크에 의하여 관리된다. 일단 기록이 이루어지면 그 블록의 데이터는 모든 후속 블록의 변경 없이는 소급하여 변경될 수 없다.¹⁸⁾

2. 블록체인 응용의 대표적 사례

블록체인 기술이 쓰인 대표적인 사례는 암호화폐 비트코인이다. 암호화폐는 달러나 원화와 같은 실물화폐와 달리 화폐를 발행하는 중앙은행이 없이 인터넷 네트워크에 P2P 방식으로 분산 저장되어 운영된다.

비트코인의 개발자 사토시 나카모토(Satoshi Nakamoto, 中本哲史)는 비트코인에서 블록체인을 사용하여 공적 거래장부로 기능하도록 함으로써 신뢰성 있는 기관 또는 중앙서버의 필요 없이 이중지급의 문제를 해결하였다. 이러한 비트코인 디자인은 다른 분야에의 응용을 위한 영감을 제공하게 되었다.

비트코인은 P2P 방식으로 작동하기 때문에 특정 관리자나 주인이 없다. 비트코인은 개인이나 회사가 아닌 여러 이용자의 컴퓨터에 분산 저장된다. 비트코인에서 만드는 거래 내역 묶음이 바로 블록이므로, 블록체인은 비트코인의 거래기록을 저장한 거래장부가 된다. 블록체인은 거래 내역을 공개하고 분산하여 관리한다는 의미에서 “공공 거래장부” 또는 “분산 거래장부”로도 불린다.¹⁹⁾

V. 전자공증

[내용 생략]

17) Marco Iansiti and Karim R. Lakhani, “The Truth About Blockchain”, Harvard Business Review, Jan.-Feb. 2017 Issue, <https://hbr.org/2017/01/the-truth-about-blockchain>: 핀테크 지원센터[핀테크 용어사전], “블록체인”, http://fintechcenter.or.kr/kor/info/term_detail.php?idx=31.

18) Wikipedia, “Blockchain”, <https://en.wikipedia.org/wiki/Blockchain>.

19) 네이버 지식백과(ICT 시사상식 2017), “블록체인”, <http://terms.naver.com/entry.nhn?docId=3586111&cid=59277&categoryId=59283>.

제 2 절 개인정보 보호 일반

I. 서 설

[1.~3. : 내용 생략]

4. 적용 법규

개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 「개인정보 보호법」이 정하는 바에 따른다^(개인 6조). 이 법은 개인정보 보호에 관하여 공적 부문과 사적 부문 모두에 적용되는 기본법의 성격을 가진다.

개인정보 보호위원회는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 "표준지침"이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다^(개인 12조 1항). 중앙행정기관의 장은 표준지침에 따라 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있고^(개인 12조 2항), 국회, 법원, 헌법재판소 및 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호지침을 정하여 시행할 수 있다^(개인 12조 3항).

한편, 개인정보 단체소송^(개인 51조)의 절차를 위하여 「개인정보 단체소송규칙」^(2011.9.28 대법원규칙 제2358호)이 제정되어 있다.

전자상거래에 관한 정보의 보호에 관하여는 「개인정보 보호법」 외에 「전자문서법」, 「전자금융거래법」, 「신용정보법」 등이 규정하고 있다. 또 전자상거래의 기초가 되는 정보통신 서비스에 관하여는 「정보통신망법」이 정보통신망의 안정성 확보 등^(45조-)과 영리목적의 광고성 정보 전송 제한^(50조) 등을 규정하고 있다.

II. 개인정보의 수집·이용 및 제공

1. 개인정보의 수집·이용

(1) 기본원칙

개인정보처리자는 개인정보를 수집하거나 그 수집 목적의 범위에서 이용하려면 원칙적으로 법 소정의 사항을 정보주체에게 알리고 정보주체의 동의를 받아야 한다(개인 15조 1항 1호·2항). 이것은 개인정보의 수집·이용에 관하여 동의접근법(consent approach)을 채택하고 있음을 밝힌 것이다.

정보주체의 동의를 받지 아니하고 개인정보를 수집한 자에게는 과태료가 부과된다(개인 75조 1항 1호).

(2) 개인정보의 수집·이용 동의

1) 수집·이용 동의의 요건 개인정보처리자는 개인정보의 수집에 관하여 정보주체의 동의를 받을 때에는 다음의 사항을 정보주체에게 알려야 한다. 다음의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다(개인 15조 2항).

- ① 개인정보의 수집·이용 목적.
- ② 수집하려는 개인정보의 항목.
- ③ 개인정보의 보유 및 이용 기간.
- ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용.

개인정보의 수집에 관하여 정보주체의 동의를 받을 때 정보주체에게 알려야 할 사항을 알리지 아니한 자에게는 과태료가 부과된다(개인 75조 2항 1호).

개인정보처리자가 정보주체의 동의를 얻지 아니하고 개인정보를 수집·이용함으로써 인하여 손해를 입으면 손해배상책임 또는 법정손해배상책임을 진다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다(개인 39조 39조의2).

2) 동의 없이 수집·이용할 수 있는 경우 개인정보처리자는 다음의 어느 하나에 해당하는 경우에는 정보주체의 동의 없이 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다(개인 15조 1항 2호-6호).

- ① 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우.
- ② 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우.
- ③ 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우.

④ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우.

⑤ 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

2. 개인정보의 제공

(1) 기본원칙

개인정보처리자는 다음의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다)할 수 있다(개인 17조).

① 정보주체의 동의를 받은 경우. 개인정보의 제공에 관하여도 원칙적으로 동의접근법을 취하고 있다.

② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우(개인 15조 1항 2호), 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우(개인 15조 1항 3호) 및 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우(개인 15조 1항 5호)에 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우.

위의 ②에 해당하지 아니함에도 위의 ①을 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자는 형사제재를 받는다(개인 71조).

(2) 개인정보 제공 동의

개인정보처리자는 개인정보 제공 동의를 받을 때에는 다음의 사항을 정보주체에게 알려야 한다. 다음의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다(개인 17조). 이 규정을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자에게는 과태료가 부과된다(개인 75조 2항 1호).

- ① 개인정보를 제공받는 자.
- ② 개인정보를 제공받는 자의 개인정보 이용 목적.
- ③ 제공하는 개인정보의 항목.
- ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간.
- ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용.

개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 위의 ① 내지 ⑤에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 「개인정보 보호법」을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다(개인 17조^{3항}).

(3) 수집·이용에 대한 동의와 구분

개인정보처리자는 「개인정보 보호법」에 따른 개인정보의 처리에 대하여 정보주체(법정대리인을 포함한다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다(개인 22조^{1항}).

또 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다(개인 22조^{3항}).

위의 규정들을 위반하여 동의를 받은 자에게는 과태료가 부과된다(개인 75조^{3항 2호}).

3. 동의를 얻는 방법

개인정보처리자는 「개인정보 보호법」에 따른 개인정보의 처리에 대하여 정보주체(법정대리인을 포함한다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다(개인 22조^{1항}).

개인정보처리자는 위의 동의를 서면(「전자문서법」 제2조 제1호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 행정안

전부령으로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다^(개인 22조 2항).

4. 개인정보의 수집·이용 및 제공 제한

(1) 개인정보의 수집 제한

1) 사생활침해의 방지 개인정보 보호는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다^(개인 3조 6항).

개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다^(개인 23조 1항 본문). 이 규정을 위반한 자는 이용자에게 손해배상책임을 지고^(개인 39조), 형사제재를 받는다^(개인 71조 3호).

2) 최소수집의 원칙 개인정보처리자는 개인정보를 수집하는 경우에는 그 목적에 필요한 범위에서 최소한의 개인정보를 수집하여야 한다^(개인 16조 1항 전단). 이것을 최소수집의 원칙이라 한다. 최소한의 개인정보 수집이라는 입증책임은 정보개인정보처리자가 부담한다^(개인 16조 1항 후단).

개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다^(개인 16조 2항).

개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 그 서비스의 제공을 거부하여서는 아니 된다^(개인 16조 3항). 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다고 할 것이다. 위의 규정을 위반하여 서비스의 제공을 거부한 자에게는 과태료가 부과된다^(개인 75조 2항 2호).

(2) 개인정보의 목적 외 이용·제공 제한

1) 제한의 원칙 개인의 사생활이 침해되는 것을 최소한으로 하기 위하여는 개인정보의 목적 외의 이용·제공을 최대한 제한할 필요가 있다. 개인정보처리자는 개인정보를 개인정보의 수집·이용에 관한 규정^(개인 15조 1항)에 따

른 범위를 초과하여 이용하거나 개인정보의 제공에 관한 규정(개인 17조)에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다(개인 18조).

위의 규정을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자는 형사제재를 받는다(개인 71조). 또 위의 규정을 위반한 자는 그 행위로 손해를 입은 이용자에게 손해배상책임을 진다(개인 39조).

2) 예 외 개인정보의 목적 외 이용·제공은 정보주체로부터 별도의 동의를 받은 때, 다른 법률에 특별한 규정이 있는 때 등의 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다(개인 18조 2항 본문). 다만, 이용자(「정보통신망법」 제2조 제1항 제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 처리하는 정보통신서비스 제공자(「정보통신망법」 제2조 제1항 제3호에 해당하는 자를 말한다. 이하 같다)의 경우 정보주체로부터 별도의 동의를 받은 때 및 다른 법률에 특별한 규정이 있는 때로 한정한다(개인 18조 2항 단서 전단).

개인정보처리자는 정보주체로부터 별도의 동의를 받은 때(개인 18조 2항 1호)에는 다음의 사항을 정보주체에게 알려야 한다. 다음의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다(개인 18조 3항).

- ① 개인정보를 제공받는 자.
- ② 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다).
- ③ 이용 또는 제공하는 개인정보의 항목.
- ④ 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다).
- ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용.

개인정보처리자는 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다(개인 18조 5항).

개인정보처리자로부터 정보주체의 개인정보를 제공받은 자는 그 정보주체의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우에는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용할 수 있다(개인_{19조}).

위의 규정들을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자는 형사제재를 받는다(개인_{2호} 71조). 또 위의 규정을 위반한 자는 그 행위로 손해를 입은 이용자에게 손해배상책임을 진다(개인_{39조}).

(3) 개인정보를 제공받은 자의 이용·제공 제한

개인정보처리자로부터 개인정보를 제공받은 자는 정보주체로부터 별도의 동의를 받거나 다른 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다(개인_{19조}). 이 규정을 위반한 자는 형사제재를 받는다(개인_{2호} 71조).

(4) 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지

개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 ① 개인정보의 수집 출처, ② 개인정보의 처리 목적, ③ 개인정보 처리의 정지(개인_{37조})를 요구할 권리가 있다는 사실을 정보주체에게 알려야 한다(개인_{1항} 20조).

위의 규정에도 불구하고 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 정보주체의 동의를 받아 정보주체 이외로부터 개인정보를 수집하여(개인_{1항} 17조) 처리하는 때에는 위의 모든 사항을 정보주체에게 알려야 한다(개인_{본문} 20조 2항). 다만, 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다(개인_{2항} 20조).

위의 두 가지 규정(개인_{2항} 20조 1항)은 다음의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 「개인정보 보호법」에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다(개인_{4항} 20조).

① 고지를 요구하는 대상이 되는 개인정보가 개인정보 보호위원회에의 등록에서 제외되는 개인정보파일(개인_{2항} 32조 각 호)에 포함되어 있는 경우.

② 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우.

(5) 개인정보의 파기

개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다(개인 21조_{1항}). 이 규정을 위반하여 개인정보를 파기하지 아니한 정보통신서비스 제공자 등은 형사제재를 받는다(개인 73조_{1항 1호}).

개인정보처리자가 위의 규정에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다(개인 21조_{2항}).

개인정보처리자가 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다(개인 21조_{3항}).

Ⅲ. 개인정보의 처리 제한

1. 민감정보의 처리 제한

1) 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 민감정보³⁰⁾를 처리하여서는 아니 된다(개인 23조_{1항 본문}). 이 규정을 위반한 자는 형사제재를 받는다(개인 71조_{3호}).

30) 다음의 어느 하나에 해당하는 정보를 말한다(개인 영 18조 1항 본문).

- ① 유전자검사 등의 결과로 얻어진 유전정보.
- ② 「형의 실효 등에 관한 법률」 제2조 제5호에 따른 범죄경력자료에 해당하는 정보.
- ③ 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보.
- ④ 인종이나 민족에 관한 정보.

다만, 공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 규정(개인 18조 2항 5호-9호)에 따라 위의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다(개인 영 18조).

예외로, 위의 규정은 ① 개인정보 수집 또는 개인정보 제공 시 정보주체에게 알려할 사항(개인 15조 2항 각 호, 17조 2항 각 호)을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우와 ② 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에는 적용하지 아니한다(개인 23조 1항 단서).

2) 개인정보처리자가 1)의 ①②에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 「개인정보 보호법」 제29조(안전조치의무)에 따른 안전성 확보에 필요한 조치를 하여야 한다(개인 23조 2항). 이 규정을 위반한 자에게는 과태료가 부과되고(개인 75조 2항 6호), 그 결과 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자는 형사제재를 받는다(개인 73조 1호).

2. 고유식별정보의 처리 제한

1) 개인정보처리자는 다음의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보³¹⁾(이하 “고유식별정보”라 한다)를 처리할 수 없다(개인 24조 1항). 이 규정을 위반하여 고유식별정보를 처리한 자는 형사제재를 받는다(개인 71조 4호).

① 정보주체에게 개인정보의 수집·이용 또는 제공 시 알려야 할 사항(개인 15조 2항 각 호, 17조 2항 각 호)을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우.

② 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우.

2) 개인정보처리자가 1)의 규정에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록

31) 다음의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 「개인정보 보호법」 제18조(개인정보의 목적 외 이용·제공 제한) 제2항 제5호부터 제9호까지의 규정에 따라 위의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다(개인 영 19조).

- ① 「주민등록법」 제7조 제3항에 따른 주민등록번호.
- ② 「여권법」 제7조 제1항 제1호에 따른 여권번호.
- ③ 「도로교통법」 제80조에 따른 운전면허의 면허번호.
- ④ 「출입국관리법」 제31조 제4항에 따른 외국인등록번호.

대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다(개인 24조 3항, 영 21조, 30조). 이 규정을 위반한 자에게는 과태료가 부과되고(개인 75조 2항 6호), 그 결과 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자는 형사제재를 받는다(개인 73조 1호).

3) 행정안전부장관은 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보 처리자가 2)의 규정에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다(개인 24조 4항). 행정안전부장관은 대통령령으로 정하는 전문기관으로 하여금 이 규정에 따른 조사를 수행하게 할 수 있다(개인 24조 5항).

3. 주민등록번호의 처리 제한

고유식별정보의 처리 제한에 관한 규정(개인 24조 1항)에도 불구하고 개인정보처리자는 다음의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다(개인 24조 2항 1호). 이 규정을 위반한 자에게는 과태료가 부과된다(개인 75조 2항 4호의2).

- ① 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우.
- ② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우.
- ③ ① 및 ②에 준하여 주민등록번호 처리가 불가피한 경우로서 행정안전부령으로 정하는 경우.

개인정보처리자는 암호화 등 안전성 확보에 필요한 조치(개인 24조 3항)에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다(개인 24조 2항 2호). 이에 따른 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다(개인 21조 2항 2호). 위의 규정을 위반하여 암

호화 조치를 하지 아니한 자에게는 과태료가 부과된다(개인 75조 2항 4호의3).

개인정보처리자는 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다(개인 24조 2항 3항). 이 규정을 위반한 자에게는 과태료가 부과된다(개인 75조 2항 5호). 행정안전부장관은 개인정보처리자가 이 규정에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다(개인 24조 2항 4항).

4. 업무위탁에 따른 개인정보의 처리 제한

개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음의 내용이 포함된 문서에 의하여야 한다(개인 26조 1항).

- ① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항.
- ② 개인정보의 기술적·관리적 보호조치에 관한 사항.
- ③ 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항.

위의 규정에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다(개인 26조 2항).

위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다(개인 26조 3항).

위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다(개인 26조 4항).

수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다(개인 26조 5항). 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 「개인정보 보호

법」을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다(개인 26조).

5. 영업양도 등에 따른 개인정보의 이전

개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다(개인 27조).

- ① 개인정보를 이전하려는 사실.
- ② 개인정보를 이전받는 자(이하 “영업양수자 등”이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처.
- ③ 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차.

영업양수자 등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 위의 규정에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다(개인 27조).

영업양수자 등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자 등은 개인정보처리자로 본다(개인 27조).

6. 개인정보취급자에 대한 감독

개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(이하 “개인정보취급자”라 한다)에 대하여 적절한 관리·감독을 행하여야 한다(개인 28조).

개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다(개인 28조).

IV. 가명정보의 처리에 관한 특례

1. 서 설

개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다(개인 28조 의2 1항). 개인정보처리자는 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다(개인 28조 의2 2항).

위의 규정에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다(개인 28조 의3 1항·3항). 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 「개인정보 보호법」의 적용이 제외되는 정보(개인 58조 의2)에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다(개인 28조 의3 2항).

2. 안전조치의무 및 금지의무

개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다(개인 28조 의4 1항).

개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다(개인 28조 의4 2항).

누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다(개인 28조 의5 1항). 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다(개인 28조 의5 2항).

3. 과징금의 부과

개인정보 보호위원회는 개인정보처리자가 가명정보 처리 시 금지의무(개인 28조 의5 1항)를 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경

우 전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억 원 또는 자본금의 100분의 3 중 큰 금액 이하로 과징금을 부과할 수 있다(개인 28조의6 1항). 과징금의 부과·징수 등에 필요한 사항은 주민등록번호의 분실 등의 경우에 관한 규정을 준용한다(개인 28조의6 2항, 34조의2 3항-5항).

4. 적용범위

가명정보는 「개인정보 보호법」 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지), 제21조(개인정보의 파기), 제27조(영업양도 등에 따른 개인정보의 이전 제한), 제34조 제1항(개인정보 유출 통지 등), 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등), 제39조의3(개인정보의 수집·이용 동의 등에 대한 특례), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례), 제39조의6(개인정보의 파기에 대한 특례), 제39조의7(이용자의 권리 등에 대한 특례), 제39조의8(개인정보 이용내역의 통지)까지의 규정을 적용하지 아니한다(개인 28조).

V. 개인정보의 안전한 관리

1. 개인정보 처리방침의 수립 및 공개

개인정보처리자는 다음의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 「개인정보 보호법」 제32조(개인정보파일의 등록 및 공개)에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다(개인 30조).

- ① 개인정보의 처리 목적.
- ② 개인정보의 처리 및 보유 기간.
- ③ 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다).
- ④ 개인정보의 파기절차 및 파기방법(「개인정보 보호법」 제21조 제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다).
- ⑤ 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다).
- ⑥ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항.

⑦ 개인정보 보호책임자^(개인 31조)의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처.

⑧ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다).

⑨ 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항.

개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다^(개인 30조, 2항).

개인정보 보호위원회는 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다^(개인 30조, 4항). 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자에게는 과태료가 부과된다^(개인 75조, 4항 7호).

개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다^(개인 30조, 3항).

2. 개인정보 보호책임자의 지정

개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 하며^(개인 31조, 1항), 이를 위반한 자에게는 과태료가 부과된다^(개인 75조, 4항 8호).

개인정보 보호책임자는 다음의 업무를 수행한다^(개인 31조, 2항).

- ① 개인정보 보호 계획의 수립 및 시행.
- ② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선.
- ③ 개인정보 처리와 관련한 불만의 처리 및 피해 구제.
- ④ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축.
- ⑤ 개인정보 보호 교육 계획의 수립 및 시행.
- ⑥ 개인정보파일의 보호 및 관리·감독.
- ⑦ 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무.

개인정보 보호책임자는 위의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다^(개인 31조, 3항).

개인정보 보호책임자는 개인정보 보호와 관련하여 「개인정보 보호법」

및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다(개인^{31조}_{4항}).

개인정보처리자는 개인정보 보호책임자가 그의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된다(개인^{31조}_{5항}).

3. 안전조치의무

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다(개인^{29조}₄ [판례]).

위의 규정을 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자는 형사제재를 받는다(개인^{73조}_{1호}).

[판례 4] 개인정보의 안전성 확보 의무

「구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2008. 2. 29. 법률 제8852호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다) 제28조 제1항은 "정보통신서비스 제공자 등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 정보통신부령이 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 조치를 하여야 한다."라고 규정하고 있다. …… 따라서 정보통신서비스 제공자는 …… 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 할 법률상 의무를 부담한다.

나아가 정보통신서비스 제공자가 정보통신서비스를 이용하려는 이용자와 정보통신서비스 이용계약을 체결하면서, 이용자로 하여금 이용약관 등을 통해 개인정보 등 회원정보를 필수적으로 제공하도록 요청하여 이를 수집하였다면, 정보통신서비스 제공자는 위와 같이 수집한 이용자의 개인정보 등이 분실·도난·누출·변조 또는 훼손되지 않도록 개인정보 등의 안전성 확보에 필요한 보호조치를 취하여야 할 정보통신서비스 이용계약상의 의무를 부담한다.³²⁾

32) 대법원 2015. 2. 12. 선고 2013다43994, 44003 판결.

3. 개인정보파일의 등록 및 공개

공공기관의 장이 개인정보파일을 운용하는 경우에는 다음의 사항을 개인정보 보호위원회에 등록하여야 한다. 등록된 사항이 변경된 경우에도 또한 같다(개인 32조 1항).

- ① 개인정보파일의 명칭.
- ② 개인정보파일의 운영 근거 및 목적.
- ③ 개인정보파일에 기록되는 개인정보의 항목.
- ④ 개인정보의 처리방법.
- ⑤ 개인정보의 보유기간.
- ⑥ 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자.

⑦ 그 밖에 대통령령으로 정하는 사항.

국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일 등에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다(개인 32조 2항 참조).

개인정보 보호위원회는 필요하면 개인정보파일의 등록사항과 그 내용을 검토하여 해당 공공기관의 장에게 개선을 권고할 수 있으며, 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다(개인 32조 3항·4항).

국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소 규칙 및 중앙선거관리위원회규칙으로 정한다(개인 32조 6항).

4. 개인정보 보호 인증

행정안전부장관은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 「개인정보 보호법」에 부합하는지 등에 관하여 인증(유효기간 3년)할 수 있다(개인 32조의 2 1항·2항). 이 규정에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다(개인 32조의 2 6항).

행정안전부장관은 개인정보 보호 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다(개인 32조의 2 4항).

개인정보 관리체계, 정보주체 권리보장, 안전성 확보조치가 이 법에 부합

하는지 여부 등 개인정보 보호 인증의 기준·방법·절차 등 필요한 사항은 대통령령으로 정한다(개인 32조^{의2 8항}).

5. 개인정보 유출 등의 통지·신고

개인정보처리자는 개인정보의 분실·도난·누출에 대한 대책을 마련하고 그 피해를 최소화할 수 있는 조치를 강구하여야 하지만, 개인정보의 분실·도난·누출이 발생한 때에는 피해를 방지 또는 최소화하기 위한 신속한 조치를 할 필요가 있다. 이에 따라 「개인정보 보호법」은 개인정보 유출 통지 등을 규정하고 있다.

개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음의 사실을 알려야 한다(개인 34조^{1항}).

- ① 유출된 개인정보의 항목.
- ② 유출된 시점과 그 경위.
- ③ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보.
- ④ 개인정보처리자의 대응조치 및 피해 구제절차.
- ⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처.

개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다(개인 34조^{2항}).

개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 위의 규정들에 따른 조치 결과를 지체 없이 개인정보 보호위원회 또는 한국인터넷진흥원에 신고하여야 한다. 이 경우 개인정보 보호위원회 또는 한국인터넷진흥원은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다(개인 34조^{3항}, 영 39조).

6. 안전조치의무

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다(개인 29조^[판례] 4).

위의 규정을 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자는 형사제재를 받는다(개인 73조. 1호).

[판례 4] 개인정보의 안전성 확보 의무

「구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2008. 2. 29. 법률 제8852호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다) 제28조 제1항은 “정보통신서비스 제공자 등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 정보통신부령이 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 조치를 하여야 한다.”라고 규정하고 있다. …… 따라서 정보통신서비스 제공자는 …… 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 할 법률상 의무를 부담한다.

나아가 정보통신서비스 제공자가 정보통신서비스를 이용하려는 이용자와 정보통신서비스 이용계약을 체결하면서, 이용자로 하여금 이용약관 등을 통해 개인정보 등 회원정보를 필수적으로 제공하도록 요청하여 이를 수집하였다면, 정보통신서비스 제공자는 위와 같이 수집한 이용자의 개인정보 등이 분실·도난·누출·변조 또는 훼손되지 않도록 개인정보 등의 안전성 확보에 필요한 보호조치를 취하여야 할 정보통신서비스 이용계약상의 의무를 부담한다.³³⁾

7. 과징금의 부과

개인정보 보호위원회는 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억 원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 안전성 확보에 필요한 조치(개인 24조. 3항)를 다한 경우에는 그러하지 아니하다(개인 34조. 2. 1항).

개인정보 보호위원회는 위의 과징금을 부과하는 경우에는 다음의 사항을 고려하여야 한다(개인 34조. 2. 2항).

- ① 안전성 확보에 필요한 조치(개인 24조. 3항) 이행 노력 정도.
- ② 분실·도난·유출·위조·변조 또는 훼손된 주민등록번호의 정도.
- ③ 피해확산 방지를 위한 후속조치 이행 여부.

33) 대법원 2015. 2. 12. 선고 2013다43994, 44003 판결.

개인정보 보호위원회는 과징금을 내야 할 자가 납부기한까지 내지 아니하면 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 내지 아니한 과징금의 연 100분의 6의 범위에서 대통령령으로 정하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다(개인 34조_{의2 3항}).

개인정보 보호위원회는 과징금을 내야 할 자가 납부기한까지 내지 아니하면 기간을 정하여 독촉을 하고, 그 지정한 기간 내에 과징금 및 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다(개인 34조_{의2 4항}).

과징금의 부과·징수에 관하여 그 밖에 필요한 사항은 대통령령으로 정한다(개인 34조_{의2 5항}).

VI. 정보주체의 권리보장

1. 개인정보의 열람

정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다(개인 35조_{1항}).

위의 규정에도 불구하고 정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정하는 바에 따라 개인정보 보호위원회를 통하여 열람을 요구할 수 있다(개인 35조_{2항}).

개인정보처리자는 개인정보의 열람을 요구받았을 때에는 대통령령으로 정하는 기간 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다(개인 35조_{3항}).

개인정보처리자는 다음의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다(개인 35조_{4항}).

- ① 법률에 따라 열람이 금지되거나 제한되는 경우.
- ② 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우.

③ 공공기관이 다음의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우.

㉠ 청소년조세의 부과·징수 또는 환급에 관한 업무.

㉡ 「초·중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무.

㉢ 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무.

㉣ 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무.

㉤ 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무.

개인정보의 열람 요구, 열람 제한, 통지 등의 방법 및 절차에 관하여 필요한 사항은 대통령령으로 정한다^(개인 35조 5항).

정보주체는 개인정보의 열람을 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다^(개인 38조).

2. 개인정보의 정정·삭제

자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다^(개인 36조 1항 본문). 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없으며^(개인 36조 1항 단서), 정보주체의 요구가 이에 해당될 때에는 개인정보처리자는 지체 없이 그 내용을 정보주체에게 알려야 한다^(개인 36조 4항).

개인정보처리자는 위의 규정에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다^(개인 36조 2항). 개인정보처리자는 이에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다^(개인 36조 5항).

개인정보처리자가 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다^(개인 36조 3항).

개인정보의 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다^(개인 36조, 6항).

정보주체는 개인정보의 정정·삭제를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다^(개인 38조).

3. 개인정보의 처리정지 등

정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다^(개인 37조, 1항).

개인정보처리자는 위의 규정에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있으며^(개인 37조, 2항), 이 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다^(개인 37조, 3항).

- ① 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우.
- ② 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우.
- ③ 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우.
- ④ 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지의사를 명확하게 밝히지 아니한 경우

개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다^(개인 37조, 4항).

개인정보 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다^(개인 37조, 5항).

정보주체는 개인정보의 처리정지를 문서 등 대통령령으로 정하는 방법·

절차에 따라 대리인에게 하게 할 수 있다^(개인 38조).

4. 손해배상책임 및 법정손해배상 청구

「개인정보 보호법」은 개인정보처리자에 대한 일반 손해배상 및 법정손해배상청구를 규정하고 있다^(개인 39조; 39조의2).

(1) 손해배상책임

정보주체는 개인정보처리자가 「개인정보 보호법」을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다^(개인 39조; 1항). 정보주체가 정개인정보처리자의 과실을 입증하는 것은 매우 어려우므로 개인정보처리자에게 증명책임을 전환한 것이다.

개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다^(개인 39조; 3항). 영미법상의 징벌적 배상 제도를 도입한 것이다.

법원은 위의 손해배상액을 정할 때에는 다음의 사항을 고려하여야 한다^(개인 39조; 4항).

- ① 고의 또는 손해 발생의 우려를 인식한 정도.
- ② 위반행위로 인하여 입은 피해 규모.
- ③ 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익.
- ④ 위반행위에 따른 벌금 및 과징금.
- ⑤ 위반행위의 기간·횟수 등.
- ⑥ 개인정보처리자의 재산상태.
- ⑦ 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도.
- ⑧ 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도.

(2) 법정손해배상의 청구

손해배상의 청구에 관한 규정(개인 39조¹항)에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다(개인 39조²항¹).

법원은 위의 규정에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 위의 규정의 범위에서 상당한 손해액을 인정할 수 있다(개인 39조²항²).

손해배상책임 규정(개인 39조)에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 위의 규정에 따른 청구(즉, 법정 손해배상의 청구)로 변경할 수 있다(개인 39조²항³).

(3) 손해배상의 보장

정보통신서비스 제공자 등은 (1) 및 (2)에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다(개인 39조³항¹).

위의 규정에 따른 가입 대상 개인정보처리자의 범위, 기준 등에 필요한 사항은 대통령령으로 정한다(개인 39조³항²).

5. 개인정보 단체소송

「소비자기본법」 제29조에 따라 공정거래위원회에 등록된 소비자단체와 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 일정한 요건을 갖춘 단체는 개인정보처리자가 「개인정보 보호법」 제49조에 따른 집단 분쟁조정을 거부하거나 집단분쟁조정 결과를 수락하지 아니한 경우에는 법원에 권리침해 행위의 금지·중지를 구하는 단체소송을 제기할 수 있다(개인 51조¹항).

단체소송의 소는 피고의 주된 사무소 또는 영업소가 있는 곳, 주된 사무소나 영업소가 없는 경우에는 주된 업무담당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다(개인 52조¹항).

원고의 청구를 기각하는 판결이 확정된 경우 이와 동일한 사안에 관하여는 「개인정보 보호법」 제51조(단체소송의 대상 등)에 따른 다른 단체는

단체소송을 제기할 수 없다. 다만, 다음의 어느 하나에 해당하는 경우에는 그러하지 아니하다^(개인 56조).

① 판결이 확정된 후 그 사안과 관련하여 국가·지방자치단체 또는 국가·지방자치단체가 설립한 기관에 의하여 새로운 증거가 나타난 경우.

② 기각판결이 원고의 고의로 인한 것임이 밝혀진 경우.

단체소송에 관하여 「개인정보 보호법」에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다^(개인 56조).

개인정보 단체소송의 세부절차에 관하여는 「개인정보 보호법」^(개인 52조 -57조)과 「개인정보 단체소송규칙」 참조.

VII. 정보통신서비스 제공자의 개인정보 처리 등 특례

2020년 2월 4일의 개정 「개인정보 보호법」은 정보통신서비스 이용자의 개인정보 보호에 관한 「정보통신망법」의 규정을 흡수하면서 정보통신서비스 제공자의 개인정보 처리 등을 특례로 규정하였다.

1. 개인정보의 수집·이용 동의 등에 대한 특례

정보통신서비스 제공자는 개인정보의 수집·이용 규정^(개인 15조)에도 불구하고 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음의 어느 하나의 사항을 변경하려는 경우에도 또한 같다^(개인 39조 의3 1항).

① 개인정보의 수집·이용 목적.

② 수집하는 개인정보의 항목.

③ 개인정보의 보유·이용 기간.

정보통신서비스 제공자는 다음의 어느 하나에 해당하는 경우에는 이용자의 동의 없이 이용자의 개인정보를 수집·이용할 수 있다^(개인 39조 의3 2항).

① 정보통신서비스(「정보통신망법」 제2조 제1항 제2호에 따른 정보통신서비스를 말한다. 이하 같다)의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우.

② 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우.

③ 다른 법률에 특별한 규정이 있는 경우

정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부해서는 아니 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다(개인 39조 의3 3항).

정보통신서비스 제공자는 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 하고, 대통령령으로 정하는 바에 따라 법정대리인이 동의하였는지를 확인하여야 한다(개인 39조 의3 4항). 정보통신서비스 제공자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 하는 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다(개인 39조 의3 5항).

개인정보 보호위원회는 개인정보 처리에 따른 위험성 및 결과, 이용자의 권리 등을 명확하게 인지하지 못할 수 있는 만 14세 미만의 아동의 개인정보 보호 시책을 마련하여야 한다(개인 39조 의3 6항).

2. 개인정보 유출 등의 통지·신고에 대한 특례

개인정보 유출 등의 통지 규정(개인 34조 의1항 3항)에도 불구하고 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자(이하 “정보통신서비스 제공자 등”이라 한다)는 개인정보의 분실·도난·유출(이하 “유출 등”이라 한다) 사실을 안 때에는 지체 없이 다음의 사항을 해당 이용자에게 알리고 개인정보 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다(개인 39조 의4 1항 본문).

- ① 유출 등이 된 개인정보 항목.
- ② 유출 등이 발생한 시점.
- ③ 이용자가 취할 수 있는 조치.
- ④ 정보통신서비스 제공자 등의 대응 조치.
- ⑤ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처.

위의 신고를 받은 대통령령으로 정하는 전문기관은 지체 없이 그 사실을 개인정보 보호위원회에 알려야 한다(개인 39조 의4 2항).

이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다^(개인 39조의4, 1항 단서). 이 경우 정보통신서비스 제공자 등은 이에 따른 정당한 사유를 보호위원회에 소명하여야 한다^(개인 39조의4 3항).

3. 개인정보의 보호조치에 대한 특례

정보통신서비스 제공자 등은 이용자의 개인정보를 처리하는 자를 최소한으로 제한하여야 한다^(개인 39조의5). 개인정보의 분실·도난·누출 등을 최소한으로 하여 정보주체가 입을 손해를 방지하기 위한 조치이다.

4. 개인정보의 파기에 대한 특례

정보통신서비스 제공자 등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다. 다만, 그 기간에 대하여 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우에는 그에 따른다^(개인 39조의6 1항).

정보통신서비스 제공자 등은 위의 기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항을 전자우편 등 대통령령으로 정하는 방법으로 이용자에게 알려야 한다^(개인 39조의6 2항).

5. 이용자의 권리 등에 대한 특례

이용자는 정보통신서비스 제공자 등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다^(개인 39조의7 1항). 정보통신서비스 제공자 등은 위의 규정에 따른 동의를 철회, 개인정보의 열람^(개인 35조), 개인정보의 정정^(개인 36조)을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다^(개인 39조의7 2항).

정보통신서비스 제공자 등은 위의 규정에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 하여야 한다^(개인 39조의7 3항).

정보주체는 위의 동의 철회 등의 요구를 문서 등 대통령령으로 정하는

방법·절차에 따라 대리인에게 하게 할 수 있다(개인 38조).

6. 개인정보 이용내역의 통지

정보통신서비스 제공자 등으로서 대통령령으로 정하는 기준에 해당하는 자는 「개인정보 보호법」 제23조, 제39조의3에 따라 수집한 이용자의 개인정보의 이용내역(같은 법 제17조에 따른 제공을 포함한다)을 주기적으로 이용자에게 통지하여야 한다. 다만, 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 그러하지 아니한다(개인 39조 1항).

위의 규정에 따라 이용자에게 통지하여야 하는 정보의 종류, 통지주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항은 대통령령으로 정한다(개인 39조 1항).

7. 손해배상의 보장

정보통신서비스 제공자 등은 「개인정보 보호법」 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다(개인 39조 1항).

위의 규정에 따른 가입 대상 개인정보처리자의 범위, 기준 등에 필요한 사항은 대통령령으로 정한다(개인 39조 2항).

8. 노출된 개인정보의 삭제·차단

정보통신서비스 제공자 등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다(개인 39조 1항).

위의 규정에도 불구하고 공중에 노출된 개인정보에 대하여 개인정보 보호위원회 또는 대통령령으로 지정한 전문기관의 요청이 있는 경우 정보통신서비스 제공자 등은 삭제·차단 등 필요한 조치를 취하여야 한다(개인 39조 2항).

9. 상호주의

국외 이전 개인정보의 보호 규정(개인 39조 12항)에도 불구하고 개인정보의 국외 이전을 제한하는 국가의 정보통신서비스 제공자 등에 대하여는 해당 국가의 수준에 상응하는 제한을 할 수 있다. 다만, 조약 또는 그 밖의 국제협정의 이행에 필요한 경우에는 그러하지 아니하다(개인 39조 13항).

제 3 절 전자상거래에 관한 정보의 보호

[I. ~ IV. : 생략]

V. 정보통신망의 안정성 확보 등

1. 정보통신망의 안정성·정보의 신뢰성 확보

(1) 안정성 및 신뢰성 확보조치

정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다(정통 45조 1항). 과학기술정보통신부장관은 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다(정통 45조 2항).

(2) 정보보호 사전점검

정보통신서비스 제공자는 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계에 정보보호에 관한 사항을 고려하여야 한다(정통 45조 2항 1항).

과학기술정보통신부장관은 법정의 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 대통령령으로 정하는 정보보호 사전점검기준에 따라 보호조치를 하도록 권고할 수 있다(정통 45조의2 2항, 영 36조의2 내지 36조의5).

(3) 집적된 정보통신시설의 보호

타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(이하 “집적정보통신시설 사업자”라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다(정통 46조 1항, 영 37조). 집적정보통신시설 사업자는 집적된 정보통신시설의 멸실, 훼손, 그 밖의 운영장애로 발생한 피해를 보상하기 위하여 대통령령으로 정하는 바에 따라 보험에 가입하여야 한다(정통 46조 2항, 영 38조).

집적정보통신시설 사업자는 다음의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단

할 수 있다(정통 46조 2항 1항).

① 집적정보통신시설을 이용하는 자(이하 “시설이용자”라 한다)의 정보시스템에서 발생한 이상현상으로 다른 시설이용자의 정보통신망 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우.

② 외부에서 발생한 침해사고로 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우.

③ 중대한 침해사고가 발생하여 과학기술정보통신부장관이나 한국인터넷진흥원이 요청하는 경우.

2. 정보보호 최고책임자의 지정

정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다(정통 45조의3 1항 본문). 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다(정통 45조의3 1항 단서, 영 36조의6). 위의 규정을 위반하여 정보보호 최고책임자의 지정을 신고하지 아니한 자에게는 과태료가 부과된다(정통 76조 1항 6의2호).

3. 정보보호 관리체계

(1) 정보보호 관리체계의 인증

과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 “정보보호 관리체계”라 한다)를 수립·운영하고 있는 자에 대하여 정보보호 관리체계 인증기준에 적합한지에 관하여 인증을 할 수 있다(정통 47조 1항). 전기통신사업자(전기 2조 8호)와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 일정한 자는 정보보호 관리체계의 인증을 받아야 한다(정통 47조 2항). 이 규정을 위반한 자에게는 과태료가 부과된다(정통 76조 1항 6의3호).

정보보호 관리체계 인증의 유효기간은 3년으로 한다. 다만, 과학기술정보통신부장관으로부터 정보보호 관리등급을 받은 경우 그 유효기간 동안 정

보보호 관리체계 인증을 받은 것으로 본다^(정통 47조 5항, 47조의5 1항). 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다^(정통 47조 9항, 52조). 이 규정을 위반하여 인증받은 내용을 거짓으로 홍보한 자에게는 과태료가 부과된다^(정통 76조 3항 7호).

(2) 개인정보보호 관리체계의 인증

방송통신위원회는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 “개인정보보호 관리체계”라 한다)를 수립·운영하고 있는 자에 대하여 개인정보보호 관리체계 인증기준에 적합한지에 관하여 인증을 할 수 있다^(정통 47조 3항 1항). 방송통신위원회는 이 규정에 따른 개인정보보호 관리체계 인증을 위하여 관리적·기술적·물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다^(정통 47조 3항 2항).

4. 이용자의 정보보호

정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있다^(정통 47조 4항 1항).

주요 정보통신서비스 제공자는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다^(정통 47조 4항 2항). 이 규정에 따른 보호조치의 요청 등에 관하여 이용약관으로 정하여야 하는 구체적인 사항은 대통령령으로 정한다^(정통 47조 4항 2항).

「소프트웨어산업 진흥법」 제2조에 따른 소프트웨어사업자는 보안에 관한 취약점을 보완하는 프로그램을 제작하였을 때에는 한국인터넷진흥원에 알려야 하고, 그 소프트웨어 사용자에게는 제작한 날부터 1개월 이내에 2회 이상 알려야 한다^(정통 47조 4항 3항).

5. 정보통신망 침해 등의 금지와 대응조치

누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다^(정통 48조 1항). 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 “악성프로그램”이라 한다)을 전달 또는 유포하여서는 아니 된다^(정통 48조 2항). 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다^(정통 48조 3항).

누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다^(정통 49조).

위의 규정들을 위반한 자는 형사제재를 받는다^(정통 70조의2, 71조 9호·10호·11호).

또 정보통신망 침입에 대하여 침해사고에 대응하기 위한 조치와 침해사고 발생의 신고^(정통 48조의2, 48조의3), 정보통신망 침해사고의 원인 분석^(정통 48조 4항) 등이 규정되어 있다.

6. 비밀 등의 보호 및 속이는 행위 금지

누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다^(정통 49조).

누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 된다^(정통 49조의2 1항). 이 규정을 위반하여 다른 사람의 개인정보를 수집한 자는 형사제재를 받는다^(정통 72조 1항 2호). 정보통신서비스 제공자는 위의 규정을 위반한 사실을 발견하면 즉시 방송통신위원회나 한국인터넷진흥원에 신고하여야 한다^(정통 49조의2 2항).

7. 영리목적의 광고성 정보 전송의 제한

(1) 서 설

헌법이 규정하는 표현의 자유는 절대적 자유가 아니며 타인의 권리를 침해하지 않는 범위 내에서 보장된다. 헌법은 언론·출판은 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하여서는 아니 된다고 명백히 밝히고 있으며^(21조 4항, 21조 4항), 국민의 자유와 권리는 헌법의 유보조항에 따라 법률로써

제한될 수 있다^(37조 2항). 그리하여 「정보통신망법」은 사생활의 자유를 침해하는 스팸메일 등을 규제하기 위하여 영리목적의 광고성 정보 전송을 제한하고, 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자가 준수하여야 할 방법 등을 규정하고 있다.

광고성 정보 전송을 규제하는 방식에는 Opt-in방식과 Opt-out방식이 있다. Opt-in방식은 광고성 메일, 문자 등을 전송할 때 수신자의 사전 동의를 얻은 경우에만 발송할 수 있도록 하는 방식이고, Opt-out방식은 광고성 메일 등을 전송할 때 수신자가 수신거부 의사를 밝히면 발송할 수 없도록 하는 방식이다. 「정보통신망법」은 Opt-in방식을 채택하고 있다.

(2) 명시적 사전 동의

1) 누구든지 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려면 원칙적으로 그 수신자의 명시적인 사전 동의를 받아야 한다^(정통 50조 1항 본문). 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려는 자는 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우에는 영리목적의 광고성 정보를 전송하여서는 아니 된다^(정통 50조 2항 33). 위의 규정들을 위반하여 영리 목적의 광고성 정보를 전송한 자에게는 과태료가 부과된다^(정통 76조 1항 7호).

“수신자의 명시적 사전 동의”가 무엇인지 의문이나, 사전에 수신자의 명시적인 수신 동意的 의사표시를 받아야 하고, 광고를 전송하는 자가 여러 종류의 서비스를 제공하는 경우에는 유형별로 서비스를 모두 고지하고 개별적으로 동의를 받아야 한다는 것을 뜻한다고 보아야 한다. 수신 동의를 얻기 위한 목적으로 문자, 이메일, 팩스 등을 전송하거나 전화를 거는 행위는 수신동의 없이 광고성 정보를 전송하는 것으로 법 위반에 해당할 수 있다.³⁴⁾

「개인정보 보호법」 제22조 제3항의 동의는 전송자가 광고성 정보를 전

33) 한국인터넷진흥원은 광고성 정보 전송 및 인터넷광고와 관련한 고충의 상담·처리 사업으로 불법스팸대응센터를 운영하고(정통 52조 3항 10호 참조) “광고성 정보 전송 및 인터넷광고와 관련한 고충의 상담·처리” 업무와 “휴대전화 광고 수신거부 서비스”를 제공하고 있다.

34) 방송통신위원회·한국인터넷진흥원, 「불법 스팸 방지를 위한 정보통신망법 안내서」(2016. 12.), 4쪽.

송하기 위해 수신자의 개인정보를 수집·이용하는 것에 대한 동의를 해당하고, 「정보통신망법」 제50조 제1항의 동의는 전송자가 보내는 광고성 정보를 수신하겠다는 것에 대한 동이에 해당하여 두 개의 동의는 구분 후 별개로 받아야 한다.

2) 예외로, 다음의 어느 하나에 해당하는 경우에는 수신자의 사전 동의를 받지 아니하고 영리목적의 광고성 정보를 전송할 수 있다(정통 50조¹항 단서).

① 재화 또는 용역(이하 “재화 등”이라 한다)의 거래관계를 통하여 수신자로부터 직접 연락처를 수집한 자가 해당 재화 등의 거래가 종료된 날부터 6개월(정통 영⁶¹조 1항) 이내에 자신이 처리하고 수신자와 거래한 것과 동종의 재화 등에 대한 영리목적의 광고성 정보를 전송하려는 경우.

② 「방문판매 등에 관한 법률」에 따른 전화권유판매자가 육성으로 수신자에게 개인정보의 수집출처를 고지하고 전화권유를 하는 경우.

위의 규정에도 불구하고 오후 9시부터 그 다음 날 오전 8시까지의 시간에 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려는 자는 그 수신자로부터 별도의 사전 동의를 받아야 한다. 다만, 전자우편의 경우에는 그러하지 아니하다(정통 50조 3항¹, 영 61조 2항). 이 규정을 위반하여 영리 목적의 광고성 정보를 전송한 자에게는 과태료가 부과된다(정통 76조¹항 7호).

3) 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려는 자는 수신자가 사전 동의, 수신거부의사 또는 수신동의 철회 의사를 표시할 때에는 해당 수신자에게 대통령령으로 정하는 바에 따라 이에 대한 처리 결과를 알려야 한다(정통 50조 7항¹, 영 62조 2항). 이 규정을 위반한 자에게는 과태료가 부과된다(정통 76조 3항¹²호의 3).

4) 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하기 위하여 수신동의를 받은 자는 그 수신동의를 받은 날부터 2년마다 광고성 정보 수신자의 수신동의 여부를 확인하여야 한다(정통 50조 8항¹, 영 62조 3항 1항). 이 규정을 위반한 자에게는 과태료가 부과된다(정통 76조 1항⁹호의 2).

(3) 전송방법

전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자는 다음의 방법을 준수하여야 한다.

1) 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자

는 대통령령으로 정하는 바에 따라 다음의 사항 등을 광고성 정보에 구체적으로 밝혀야 한다(정통 50조 4항, 영 61조 3항 및 별표 6).

① 전송자의 명칭 및 연락처.

② 수신자의 거부 또는 수신동의의 철회 의사표시를 쉽게 할 수 있는 조치 및 방법에 관한 사항.

위의 규정을 위반하여 광고성 정보를 전송할 때 밝혀야 하는 사항을 밝히지 아니하거나 거짓으로 밝힌 자에게는 과태료가 부과된다(정통 76조 1항 8호).

2) 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자는 다음의 어느 하나에 해당하는 조치를 하여서는 아니 된다(정통 50조 5항). 이 규정을 위반하여 조치를 한 자는 형사제재를 받는다(정통 74조 1항 4호).

① 광고성 정보 수신자의 수신거부 또는 수신동의의 철회를 회피·방해하는 조치.

② 숫자·부호 또는 문자를 조합하여 전화번호·전자우편주소 등 수신자의 연락처를 자동으로 만들어 내는 조치.

③ 영리목적의 광고성 정보를 전송할 목적으로 전화번호 또는 전자우편주소를 자동으로 등록하는 조치.

④ 광고성 정보 전송자의 신원이나 광고 전송 출처를 감추기 위한 각종 조치.

⑤ 영리목적의 광고성 정보를 전송할 목적으로 수신자를 기망하여 회신을 유도하는 각종 조치.

정보통신서비스 제공자는 영리목적의 광고성 정보가 보이도록 하거나 개인정보를 수집하는 프로그램을 이용자의 컴퓨터나 그 밖에 휴대인터넷·휴대전화 등과 같이 정보통신망에 연결되어 정보를 송수신 할 수 있는 정보처리장치에 설치하려면 이용자의 동의를 받아야 한다. 이 경우 해당 프로그램의 용도와 삭제방법을 고지하여야 한다(정통 50조의 5, 영 63조). 이 규정을 위반한 자에게는 과태료가 부과된다(정통 76조 1항 10호).

3) 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자는 수신자가 수신거부나 수신동의의 철회를 할 때 발생하는 전화요금 등의 금전적 비용을 수신자가 부담하지 아니하도록 대통령령으로 정하는 바에 따라 필요한 조치를 하여야 한다(정통 50조 6항). 이에 따라 영리목적의 광고성 정보

를 전송하는 자는 「정보통신망법」 별표 6에서 정하는 바에 따라 수신거부 및 수신동의 철회용 무료전화서비스 등을 해당 정보에 명시하여 수신자에게 이를 제공하여야 한다(정통령_{62조}). 위의 규정을 위반한 자에게는 과태료가 부과된다(정통 76조_{1항 9호}).

(4) 전송위탁

영리목적의 광고성 정보의 전송을 타인에게 위탁한 자는 그 업무를 위탁받은 자가 영리목적의 광고성 정보 전송 제한의 규정(정통_{50조})을 위반하지 아니하도록 관리·감독하여야 한다(정통 50조_{의3 1항}). 영리목적의 광고성 정보의 전송을 위탁받은 자는 그 업무와 관련한 법을 위반하여 발생한 손해의 배상책임에 있어 정보 전송을 위탁한 자의 소속 직원으로 본다(정통 50조_{의3 2항}).

(5) 게시의 제한

누구든지 영리목적의 광고성 정보를 인터넷 홈페이지에 게시하려면 인터넷 홈페이지 운영자 또는 관리자의 사전 동의를 받아야 한다. 다만, 별도의 권한 없이 누구든지 쉽게 접근하여 글을 게시할 수 있는 게시판의 경우에는 사전 동의를 받지 아니한다(정통 50조_{의7 1항}). 영리목적의 광고성 정보를 게시하려는 자는 위의 규정에도 불구하고 인터넷 홈페이지 운영자 또는 관리자가 명시적으로 게시 거부사를 표시하거나 사전 동의를 철회한 경우에는 영리목적의 광고성 정보를 게시하여서는 아니 된다(정통 50조_{의7 2항}). 위의 규정들을 위반하여 인터넷 홈페이지에 영리목적의 광고성 정보를 게시한 자에게는 과태료가 부과된다(정통 76조_{1항 11호}).

인터넷 홈페이지 운영자 또는 관리자는 위의 규정들을 위반하여 게시된 영리목적의 광고성 정보를 삭제하는 등의 조치를 할 수 있다(정통 50조_{의7 3항}).

(6) 불법행위를 위한 전송의 금지

누구든지 정보통신망을 이용하여 「정보통신망법」 또는 다른 법률에서 금지하는 재화 또는 서비스에 대한 광고성 정보를 전송하여서는 아니 된다(정통 50조_{의8}). 이 규정은 법률이 금지하는 광고성 정보를 전송하지 못하도록 하여 불법행위를 방지하기 위한 것이다.

(7) 그 밖의 규정

그 밖에도 「정보통신망법」은 광고성 정보 전송 의무 제공 등의 제한, 영리목적의 광고성 프로그램 등의 설치, 영리목적의 광고성 정보 전송차단 소프트웨어의 보급 등을 규정하고 있다^(정통 50조의3, -50조의6).