개정 「정보통신망법」 중 개인정보보호 규정 안내서

('14.5.28. 개정, '14.11.29. 시행)

2015. 2.

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

[목 차]

Ⅰ 정보통신망법의 개정 배경 및 내용

1. 개정 배경

최근 은행, 카드사 등에서 1억 건이 넘는 개인정보가 유출되는 사건이 발생하는 등 개인정보 누출사고가 지속적으로 발생하고 있습니다. 특히 정보통신망을 통한 개인정보 유출은 그 피해 정도가 지대하며, 유출된 개인정보는 2차 피해 발생 가능성도 높아 사전에 개인정보가 유출되지 못하도록 법적 제도적 장치를 마련할 필요성이 크므로, 개인정보보호 조치를 강화함과 동시에 동 법상의 의무위반에 대한 정보통신서비스 제공자의 처벌을 엄격히 하고, 법정손해배상제도를 도입하는 등 이용자 권리 구제 수단을 보완하여 이용자의 권리보호를 위한 각종 조치를 마련할 필요성이 요구되었습니다.

2. 주요 개정 내용

정보통신망법의 개정으로 개인정보보호와 관련하여서는 총10개 조문이 개정·신설되었습니다. 주요 개정 내용은 다음과 같습니다.

① 이용자의 사전 동의가 있더라도 수집 가능한 개인정보를 필요한 최소한으로 하도록 한정하고 필요한 최소한의 개인정보에 대한 개념을 명확하게 하였습니다.(법 제23조)

② 이용자의 동의 없이 개인정보 취급위탁을 할 수 있는 예외를 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 경우 외에 ‘이용자 편의 증진 등을 위하여 필요한 경우’를 추가하였습니다.(법 제25조제2항)

③ 영업양수 등의 개인정보 이전 사실을 반드시 이용자에게 통지하도록 강화하였습니다. (법 제26조제2항)

④ 실효성이 미흡한 개인정보 취급방침의 전자적 표시의무를 폐지하였습니다. (영 제14조제3항)

⑤ 신고기관에 한국인터넷진흥원을 추가하고, 누출신고 시점인 ‘누출을 안 때에 지체 없이’의 기준을 24시간 이내로 법률로 명확히 하고 통지 및 신고를 24시간 내에 하지 못한 경우 정당한 사유를 지체없이 방송통신위원회에 서면으로 소명하도록 하였습니다.(법 제27조의3 제1항, 영 제14조의2제5항)

⑥ 바이오정보를 일방향 암호화 대상에서 암호화 대상으로 하고 그밖에 암호화 대상 정보를 고시에 위임하였습니다. (영 제15조제4항)

⑦ 개인정보 파기는 복구·재생할 수 없도록 하고, 미파기시 처벌 강화하였습니다. (제29조제1항, 제73조제1호의2 신설)

⑧ 서비스를 이용하지 않는 이용자의 개인정보의 파기 등 필요한 조치를 취해야 하는 유효기간을 3년에서 1년으로 단축하였습니다. (영 제16조제1항)

⑨ 위법한 개인정보 분실·도난·누출에 대한 법정손해배상 제도를 도입하였고 법정손해배상의 청구기간은 이용자가 누출통지를 받은 날부터 3년, 누출된 날부터 10년으로 하였습니다.(제32조의2 신설)

⑩ 과징금 상한을 높이고 개인정보 분실 등의 경우 보호조치 위반에 대해 매출액 기준으로 통일하는 한편, 수탁자가 개인정보보호 규정을 위반한 경우 위탁자에게 과징금 부과 하도록 신설하였고, 개인정보 누출과 기술적·관리적 보호조치 위반과의 인과관계 입증 없이 과징금 부과하도록 하였습니다. (법 제64조의3)

Ⅱ 개정 내용 및 해설

1 필요한 최소한의 개인정보 개념 명확화

◎ 개정 내용 ◎

정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위하여 필요한 범위에서 최소한의 개인정보만 수집하여야 합니다. “이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보를 말한다”는 규정(법 제23조제3항)이 신설되었습니다.

◎ 법령 ◎

법률

제23조(개인정보의 수집 제한 등) ① 정보통신서비스 제공자는 사상, 신념, 가족 및 친인척 관계, 학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다.

② 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 범위에서 최소한의 개인정보만 수집하여야 한다.

③ 정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.

◎ 해설 ◎

❍ 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위하여 필요한 최소한의 정보만 수집하여야 하는데, ‘필요한 최소한의 정보’가 무엇인지 명확하지 않았습니다. 이에 이번 개정으로 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보를 말한다는 규정이 신설 되었습니다.

❍ 수집하는 개인정보의 항목을 필수동의 항목과 선택동의 항목으로 구분하여 최소한의 개인정보만을 수집·보관해야 하며, 필수동의 항목은 사업자가 이용자에게 서비스 제공을 위해 필수적으로 동의할 것을 요구할 수 있는 개인정보 항목으로, 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보에 한정해야 합니다.

※ (예시) 필수동의 항목과 선택동의 항목의 구분

구분	필수동의 항목	선택동의 항목
개념	· 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보 · 이용자에게 필수적 동의 요구 가능	· 사업자의 필요에 의해 수집하는 정보 · 이용자가 동의 여부를 선택 가능
예시	① 인터넷 회원제 서비스 · (본질적 기능) 회원 식별정보 · (예시) 아이디, 비밀번호, 이름, 법정 생년월일, 휴대전화번호, 이메일 등 ② 온라인 결제 서비스 · (본질적 기능) 온라인 결제 · (예시) 결제정보(카드번호, 계좌번호 등) ③ 이동통신 서비스 · (본질적 기능) 휴대전화 통화 · (예시) 이름, 연락처, 법정 생년월일, 결제정보(후불제) 등	① 인터넷 회원제 서비스 · (선택적 기능) 상품 마케팅 · (예시) 마케팅 목적의 휴대전화번호· 이메일 등 ② 온라인 결제 서비스 · (선택적 기능) 결제 알림 서비스 · (예시) 휴대전화번호, 이메일 등 ③ 이동통신 서비스 · (선택적 기능) 멤버쉽 할인 · (예시) 멤버쉽 정보(타사 이용정보)

❍ ‘해당 서비스’는 사업자가 이용자에게 정보통신망을 통해 이용약관 등에 따라 제공하는 개별 서비스를 말하며, 사업자와 이용자가 서비스 제공·이용 과정에서 합리적으로 예상 가능한 개별 서비스를 의미 합니다.

※ (예시) ① 포털 사업자 : 인터넷 회원제 서비스, 검색서비스, 게임서비스, 커뮤니티 서비스, 메일서비스 등, ② 이동통신 사업자 : 전화통화 서비스 등

❍ ‘본질적 기능’은 사업자가 해당 서비스 제공 과정에서 업무처리를 위해 반드시 필요한 기능을 의미 합니다.

※ (예시) 해당 서비스의 본질적 기능

해당 서비스	본질적 기능
인터넷 회원제 서비스	· 회원에 대한 요금조회, 상담(전화, 인터넷 등), 서비스 신청, 포인트 적립 등 · 명의도용·부정이용 방지 등 회원관리
유료 서비스	· 구매한 서비스 및 상품 결제
결재 및 배송 서비스	· 구매한 서비스 및 상품 결재, 배송
이동통신 서비스	· 휴대전화 개통-서비스 제공-이용요금 정산-고객민원 상담 등 · 가입의사 확인·명의도용 방지 등 고객관리
SNS서비스	· 통신 및 정보전달 · 친구추천 등
서비스 제공 과정에서의 법령 상 의무이행	· 정당한 이용자인지 여부 확인 · 연령에 따른 제한이 있는 경우 연령 확인

※ 자세한 사항은 방송통신위원회 "온라인 개인정보 취급 가이드라인(2014.11.12.)"을 참고하시기 바랍니다.

2 개인정보의 취급위탁시 동의 예외 요건 강화

◎ 개정 내용 ◎

정보통신망법 개정에 따라 정보통신서비스 제공자는 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우를 제외하고는 취급위탁사항에 대하여 이용자에게 고지하고 동의절차를 거쳐야 합니다. 따라서 계약을 이행하기 위한 취급위탁에 해당하더라도, 이용자 편의 증진 등을 위하여 필요한 경우에 해당하지 않는 경우에는 이용자에게 고지하고 동의를 받아야 합니다.

◎ 법령 ◎

법률

제25조(개인정보의 취급위탁) ① 정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집·보관·처리·이용·제공·관리·파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보 취급위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 개인정보 취급위탁을 받는 자(이하 "수탁자"라 한다)
2. 개인정보 취급위탁을 하는 업무의 내용

② 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 취급위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

③ 정보통신서비스 제공자등은 개인정보 취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다.

④ 정보통신서비스 제공자등은 수탁자가 이 장의 규정을 위반하지 아니하도록 관리·감독하여야 한다.

⑤ 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자등의 소속 직원으로 본다.

시행령

제10조(개인정보취급위탁의 통지) 법 제25조제2항 전단에서 "대통령령으로 정하는 방법"이란 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법을 말한다.

◎ 해설 ◎

❍ 계약의 이행을 위한 경우는 객관적으로 판단이 가능하나, 이용자의 편의 증진 등을 위한 경우에 해당하는지 여부는 객관화하기 어려운 측면이 존재하므로 이는 정보통신서비스 제공자등과 이용자가 처한 당시의 환경에 따라 다르게 평가될 수 있습니다.

❍ 현재의 상태 또는 환경을 기준으로 이전과 비교하여 서비스의 비용이나 시간이 이용자에게 유리하게 변경되었거나 계약조건이 향상되었다면 편의 증진 등을 위한 경우에 해당한다고 판단할 수 있습니다.

❍ 또한, 위탁자가 비용절감 등을 위해 위탁하는 경우에도, 이것을 이용자의 편의 증진과 관련이 있다고 볼 수 있는지 여부를 판단함에 있어서는 역시 위와 같은 기준으로 판단하여야 합니다. 그러므로 위탁자에 이익이 되는 동시에 이용자의 편의 증진 등이 되었다고 볼 수 있다면, 이용자에 고지 및 동의절차를 거치지 아니할 수 있습니다.

❍ 과거에는 계약이행을 위한 경우에 해당하면 이용자의 동의 없이 위탁이 가능하였으나, 이제는 이용자의 편의 증진을 위한 경우에 해당하는지 여부도 함께 고려해야 하므로 수탁자를 선정함에 있어서 ‘이용자의 편의’를 고려할 주의의무가 추가되었다고 볼 수 있습니다. 따라서 단순히 비용절감 차원에서 위탁 여부를 결정하는 것이 아니라, 해당 위탁으로 인해 이용자의 편의가 증진되었는지 여부를 반드시 고려해야 할 것입니다.

❍ 이용자가 취급위탁에 대한 동의를 거부하면 서비스 제공자체가 불가능하다면 이는 신속한 계약이행과 그에 따른 이용자의 편의 증진 등을 위하여 필요한 경우에 해당할 수 있습니다.

3 영업양수자등의 통지의무 강화

◎ 개정 내용 ◎

영업양수자등은 개인정보를 이전받으면 지체 없이 그 사실 및 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알리도록 개정되었습니다.

◎ 법령 ◎

법률

제26조(영업의 양수 등에 따른 개인정보의 이전) ① 정보통신서비스 제공자등이 영업의 전부 또는 일부의 양도·합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에는 미리 다음 각 호의 사항 모두를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다.

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다. 이하 이 조에서 같다)·주소·전화번호 및 그 밖의 연락처
3. 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차

② 영업양수자등은 개인정보를 이전받으면 지체 없이 그 사실 및 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다.

③ 영업양수자등은 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제공할 수 있는 당초 목적의 범위에서만 개인정보를 이용하거나 제공할 수 있다. 다만, 이용자로부터 별도의 동의를 받은 경우에는 그러하지 아니하다.

시행령

제11조(영업의 양도 등에 따른 개인정보 이전 시의 통지) ① 법 제26조제1항 각 호 외의 부분 및 제2항 본문에서 "대통령령으로 정하는 방법"이란 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법을 말한다.

② 정보통신서비스 제공자 등 또는 영업양수자 등이 과실 없이 이용자의 연락처를 알 수 없는 경우에 해당되어 제1항의 방법에 따라 통지할 수 없는 경우에는 인터넷 홈페이지에 최소 30일 이상 게시하여야 한다.

③ 천재·지변이나 그 밖에 정당한 사유로 제2항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 둘 이상의 일반일간신문(이용자의 대부분이 특정지역에 거주하는 경우에는 그 지역을 보급구역으로 하는 일반일간신문)에 1회 이상 공고하는 것으로 갈음할 수 있다.

◎ 해설 ◎

❍ 정보통신서비스 제공자등이 영업의 전부 또는 일부의 양도·합병 등으로 이용자의 개인정보를 이전하는 경우에는 개인정보를 이전하려는 사실, 개인정보를 이전받는 자의 성명·주소·전화번호 그 밖의 연락처, 이용자가 개인정보의 이전을 원하지 않는 경우 그 동의를 철회할 수 있는 방법과 절차 등을 이용자에게 알려야 합니다.

❍ 영업양수자등은 개인정보를 이전받으면 지체 없이 그 사실 및 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 합니다.

❍ 기존에는 정보통신서비스 제공자등(영업양도자)이 이용자에게 통지를 한 경우 영업양수자등은 이용자 통지의무가 없었으나, 개정 법률은 정보통신서비스 제공자등(영업양도자)이 이용자에게 통지를 했는지 여부와 상관없이 영업양수자등도 이용자에게 통지를 하도록 규정하고 있습니다.

4 개인정보 취급방침의 전자적 표시의무 폐지

◎ 개정 내용 ◎

정보통신서비스 제공자등이 개인정보 취급방침을 공개하는 경우에는 이용자가 인터넷을 통하여 개인정보취급방침의 주요 사항을 언제든지 쉽게 확인할 수 있도록 하기 위하여 방송통신위원회가 정하여 고시하는 방법에 따른 전자적 표시도 함께 하여야 한다는 규정이 폐지되었습니다.

◎ 법령 ◎

법률

제27조의2(개인정보 취급방침의 공개) ① 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 경우에는 개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

② 제1항에 따른 개인정보 취급방침에는 다음 각 호의 사항이 모두 포함되어야 한다.

1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법
2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(제29조제1항 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보 취급위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 취급방침에 포함한다)
5. 이용자 및 법정대리인의 권리와 그 행사방법
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
7. 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

③ 정보통신서비스 제공자등은 제1항에 따른 개인정보 취급방침을 변경하는 경우에는 그 이유 및 변경내용을 대통령령으로 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다.

시행령

제14조(개인정보취급방침의 공개 방법 등) ① 법 제27조의2제1항에 따라 정보통신서비스 제공자등은 개인정보의 수집 장소와 매체 등을 고려하여 다음 각 호 중 어느 하나 이상의 방법으로 개인정보취급방침을 공개하되, 그 명칭을 '개인정보취급방침'이라고 표시하여야 한다.

1. 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 법 제27조의2제2항 각 호의 사항을 이용자가 볼 수 있도록 하는 방법. 이 경우 정보통신서비스 제공자등은 글자 크기, 색상 등을 활용하여 이용자가 개인정보취급방침을 쉽게 확인할 수 있도록 표시하여야 한다.
2. 점포·사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하여 열람하도록 하는 방법
3. 동일한 제호로 연 2회 이상 계속적으로 발행하여 이용자에게 배포하는 간행물·소식지·홍보지·청구서 등에 지속적으로 게재하는 방법

② 법 제27조의2제3항에 따른 개인정보취급방침의 변경 이유 및 내용은 다음 각 호의 방법 중 어느 하나 이상의 방법으로 공지한다.

1. 정보통신서비스 제공자등이 운영하는 인터넷 홈페이지의 첫 화면의 공지사항란 또는 별도의 창을 통하여 공지하는 방법
2. 서면·모사전송·전자우편 또는 이와 비슷한 방법으로 이용자에게 공지하는 방법
3. 점포·사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하는 방법

◎ 해설 ◎

❍ 전자적 표시 의무는 이용자들이 웹사이트의 개인정보취급방침을 보다 손쉽게 확인할 수 있도록 하기 위해 도입되었습니다. 그러나 이용자가 이를 확인하기 위해서는 별도의 소프트웨어를 이용해야 하는 불편이 있어 이를 이용하는 사람이 거의 없는 반면, 정보통신서비스 제공자등에게는 과도한 부담을 발생 시키고 있었습니다.

❍ 이에 전자적 표시 의무는 실효성이 미흡한 규제로 판단하여 이번 정보통신망법 시행령의 개정으로 폐지하게 되었습니다.

❍ 앞으로 정보통신서비스 제공자등은 인터넷 홈페이지 등에 개인정보취급방침을 공개하면 되고, 전자적 표시는 하지 않아도 됩니다.

※ 개인정보 취급방침의 전자적 표시와 인터넷 홈페이지 공개는 전혀 다른 것입니다. 개인정보 취급방침의 전자적 표시는 개인정보 취급방침에 포함되어야 할 사항을 W3C(World Wide Web Consortium)에서 제정한 P3P(Platform for Privacy Preferences)의 표준 데이타 및 XML 구문 형식에 따라 작성하는 것을 말합니다. 따라서, 인터넷 홈페이지에 개인정보 취급방침을 공개할 의무가 폐지된 것으로 오해하면 안됩니다.

5 개인정보 누출 통지·신고 기한 명확화 등

◎ 개정 내용 ◎

정보통신서비스 제공자등은 개인정보 분실 · 도난 · 누출(이하 “누출등”이라 합니다)의 사실을 안 때에는 지체 없이 누출등이 된 개인정보 항목, 누출등이 발생한 시점 등을 해당 이용자에게 통지하고 방송통신위원회 또는 한국인터넷 진흥원에 신고하여야 하며, 통지 및 신고 시점이 정당한 사유 없이 24시간을 경과하여서는 안됩니다. 또한 24시간을 경과하여 통지 및 신고를 한 경우에는 정당한 사유를 방송통신위원회에 서면(전자문서 포함)으로 소명하여야 합니다.

◎ 법령 ◎

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.

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 방

송통신위원회 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.

◎ 해설 ◎

❍ 정보통신서비스 제공자등은 정당한 사유 없이 이용자에 대한 통지 및 방송통신위원회에 대한 신고가 개인정보의 누출등을 안 때부터 24시간을 경과하여서는 안됩니다.

- 이용자에 대한 통지 지연의 정당한 사유의 예시
  · 수사상의 이유 (ex. 경찰이 이용자 통지에 대해 보류를 요청한 경우)
  · 물리적·기술적·관리적인 사유로 통지가 불가능한 경우
  · 그 밖에 단전, 홍수, 폭설 등의 천재지변으로 인해 24시간 내에 통지가 불가능한 경우

- 방송통신위원회 또는 한국인터넷진흥원에 대한 신고 지연의 정당한 사유의 예시
  · 단전, 홍수, 폭설 등의 천재지변으로 인해 24시간 내에 신고가 불가능한 경우

❍ 또한, 24시간 내에 통지 및 신고를 완료하였더라도 그 내용이 허위로 작성되었거나 고의로 법정사항을 누락한 경우에는 본 조항 위반에 해당할 수 있습니다.

❍ 정보통신서비스 제공자등은 개인정보 누출등의 사실을 안 때에는 다음의 항목 모두를 이용자에게 통지 및 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 합니다.

① 누출등이 된 개인정보 항목
② 누출 등이 발생한 시점
③ 이용자가 취할 수 있는 조치
④ 정보통신서비스 제공자등의 대응 조치
⑤ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

❍ 시행령 제14조의2제2항은 위의 항목 ① 또는 ②에 관한 구체적인 내용이 확인되지 아니하였으면 그때까지 확인된 내용과 ③부터 ⑤까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하도록 규정하고 있습니다.

- 따라서 24시간 내에 진행된 통지 및 신고 내용 중 항목 ①과 ②가 미흡하다는 사유만으로는 위법하다 할 수 없으나 이에 대하여는 추후에 해당 내용을 보충하여 가능한 빠른 시일 내에 통지 및 신고하여야 합니다.

- ③부터 ⑤까지의 항목은 정당한 사유가 없는 한 24시간 내에 충실하게 통지 및 신고하여야 하며, 이를 부실하게 한 경우에는 본 조항 위반으로 볼 수 있습니다.

6 개인정보의 암호화 대상 개선

◎ 개정 내용 ◎

일방향 암호화 대상이었던 바이오정보를 암호화 대상으로 변경하고, 암호화 대상 정보를 방송통신위원회 고시에 위임하도록 개정되었습니다.

◎ 법령 ◎

법률

제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.

시행령

제15조(개인정보의 보호조치) ① 법 제28조제1항제1호에 따라 정보통신서비스 제공자등은 개인정보의 안전한 취급을 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다.

1. 개인정보 관리책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항
2. 개인정보취급자의 교육에 관한 사항
3. 제2항부터 제5항까지의 규정에 따른 보호조치를 이행하기 위하여 필요한 세부 사항

② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다.

1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행
2. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영
3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단

4. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영
5. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

③ 법 제28조제1항제3호에 따라 정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독
2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관

④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

1. 비밀번호의 일방향 암호화 저장
2. 주민등록번호, 계좌정보 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다) 등 방송통신위원회가 고시하는 정보의 암호화 저장
3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치
4. 그 밖에 암호화 기술을 이용한 보안조치

⑤ 법 제28조제1항제5호에 따라 정보통신서비스 제공자등은 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성 프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다.

⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

◎ 해설 ◎

❍ 바이오정보는 비밀번호와 달리 일방향 암호화를 하면 활용이 곤란하다는 문제점을 반영하여 암호화가 가능하도록 변경하였습니다.

❍ 또한, 현실여건의 변화에 따라 즉각적인 대응이 가능하도록 암호화 대상 개인정보를 방송통신위원회 고시에 위임하였습니다.

❍ 여기서 말하는 방송통신위원회 고시는 개인정보의 기술적·관리적 보호조치 기준을 의미합니다. 현행 고시 제6조제2항은 주민등록번호, 신용카드번호, 계좌번호를 암호화 하도록 규정하고 있으나, 시행령 개정에 따라 고시 개정을 추진하고 있으며, 운전면허번호, 외국인등록번호, 여권번호 등 고유식별번호가 추가될 예정입니다.

7 개인정보 파기의무 및 처벌 강화

◎ 개정 내용 ◎

정보통신서비스 제공자등은 개인정보의 수집·이용 목적을 달성했거나, 보유 및 이용 기간이 끝난 경우 등에는 지체 없이 개인정보를 복구·재생할 수 없도록 파기하여야 합니다. 이를 위반한 경우 2년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 처벌이 강화되었습니다.

◎ 법령 ◎

법률

제29조(개인정보의 파기) ① 정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 해당 개인정보를 복구·재생할 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

② 정보통신서비스 제공자등은 정보통신서비스를 대통령령으로 정하는 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다.

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1의2. 제29조제1항을 위반하여 개인정보를 파기하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

◎ 해설 ◎

❍ 정보통신서비스 제공자등은 개인정보의 파기 사유(목적 달성・보유기간 종료, 이용자 파기 요청 등) 발생 시에는 지체 없이 복구·재생할 수 없도록 파기하여야 합니다.

❍ 복구·재생할 수 없도록 파기한다는 것은 사회통념상 현재의 기술 수준에서 적절한 비용이 소요되는 방법을 이용하여 파기하는 것을 의미합니다.

- 인쇄물 등 파쇄가 가능한 형태인 경우에는 분쇄기 등을 이용하여 재조합이 불가능하도록 물리적으로 파쇄하거나 소각하여야 합니다.

- 하드디스크, CD/DVD, USB메모리 등의 매체에 전자기적으로 기록된 개인정보는 다시 재생시킬 수 없는 기술적 방법으로 삭제하거나 물리적인 방법으로 매체를 파괴하여 복구할 수 없도록 하여야 합니다.

☞ **복구·재생할 수 없는 파기 방법(예시)**

1. 하드 디스크 등 매체 전체의 데이터를 파기하는 경우

1) 프로그램을 이용한 파기

① 하드디스크, USB 메모리의 경우 '로우레벨포멧(Low level format)' 방법으로 파기
※ 로우레벨포멧 : 하드디스크를 공장에서 나온 초기상태로 만들어주는 포맷

② 0, 1 혹은 랜덤한 값으로 기존 데이터를 여러 번 덮어씌우는 와이핑(Wiping) 방법으로 파기

2) 물리적인 파기

① 데이터가 저장되는 디스크 플레터에 강력한 힘으로 구멍을 내어 복구가 불가능하도록 하는 천공 방법으로 파기

② CD/DVD의 경우 가위 등으로 작은 입자로 조각 내거나, 전용 CD파쇄기나 CD 파쇄가 가능한 문서파쇄기 등을 이용하여 파기

③ 고온에 불타는 종류의 매체는 소각하는 방법으로 파기

④ 자기장치를 이용해 강한 자기장으로 데이터를 복구 불가능하게 하는 디가우저(Degausser) 파기

2. 고객 서비스에 이용 중인 DB서버에 저장된 일부 데이터를 파기하는 경우

① 서비스 중인 DB의 해당 개인정보 위에 임의의 값(Null값 등)을 덮어쓰기한 후 삭제(delete)

② DB의 특정부분에 덮어쓰기가 곤란한 경우에는 테이블 데이터에 대한 논리적인 삭제(delete)도 허용되나, 신속하게 다른 데이터로 덮어쓰기(overwriting)될 수 있도록 운영

8 개인정보 유효기간 단축

◎ 개정 내용 ◎

정보통신서비스제공자 등은 이용자의 개인정보를 보호하기 위해 1년 동안 서비스를 이용하지 아니하는 이용자의 개인정보는 파기 등 필요한 조치를 취하여야 합니다.

◎ 법령 ◎

법률

제29조(개인정보의 파기)

② 정보통신서비스 제공자등은 정보통신서비스를 대통령령으로 정하는 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다.

시행령

제16조(개인정보의 파기 등) ① 법 제29조제2항에서 "대통령령으로 정하는 기간"이란 1년을 말한다. 다만, 다음 각 호의 경우에는 해당 호에 따른 기간으로 한다.

1. 다른 법령에서 별도의 기간을 정하고 있는 경우: 해당 법령에서 정한 기간
2. 이용자의 요청에 따라 기간을 달리 정한 경우: 달리 정한 기간

② 정보통신서비스 제공자등은 이용자가 정보통신서비스를 제1항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

③ 정보통신서비스 제공자등은 제2항에 따라 개인정보를 별도로 저장·관리하는 경우에는 법 또는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 해당 개인정보를 이용하거나 제공하여서는 아니 된다.

④ 정보통신서비스 제공자등은 제1항의 기간 만료 30일 전까지 개인정보가 파기되거나 분리되어 저장·관리되는 사실과 기간 만료일 및 해당 개인정보의 항목을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알려야 한다.

◎ 해설 ◎

❍ 개정 법률 이전의 경우, 정보통신서비스 제공자 등은 3년 동안 서비스를 이용하지 아니하는 이용자의 개인정보는 파기 등 필요한 조치를 취하여야 했으나, 정보통신서비스의 특성을 고려할 때 3년은 지나치게 장기간이라는 지적에 따라 개인정보 유효기간을 1년으로 단축하였습니다.

가. 개인정보의 파기 또는 분리 저장·관리 조치를 취해야 하는 서비스 미이용 기간(1년)

❍ 개인정보의 파기 또는 분리 저장·관리 조치를 취해야 하는 사유가 되는 서비스 미이용 기간은 별도의 예외 사유가 없다면 법령에 따라 1년입니다.

- 이와 관련해서 개인정보의 서비스 미이용 기간, 해당 기간 경과 후 조치사항 등 동 제도와 관련된 내용을 이용약관 등에 추가·반영하고, 변경된 내용을 이용자에게 알리는 등의 조치가 필요합니다.

나. 1년 서비스 미이용 기간의 예외

❍ 다른 법령에서 별도의 기간을 정하고 있거나 이용자의 요청에 따라 기간을 달리 정한 경우에는 1년 이외의 기간으로 서비스 미이용 기간을 정할 수 있습니다.

❍ 다른 법령에서 별도의 기간을 정한 경우

- 통신비밀보호법, 전자상거래 등에서의 소비자보호에 관한 법률 등과 같이 개별 법령에서 개인정보의 보존기간을 별도로 정하거나,

- 국세기본법, 상법 등에서처럼 법령상의 책임이나 의무를 준수하기 위해 별도의 기간(소멸시효 등)을 명시한 경우가 이에 해당됩니다.

- 따라서 캐쉬백, 포인트, 마일리지 등의 제도를 운영하고 있는 정보통신서비스 제공자등도 상법상 상사채권 소멸시효(5년)에 따른 개인정보 유효기간을 별도로 적용할 수 있습니다.

< 참고 : 개인정보의 보존기간이 명시된 법령 예시 >

근거법령	개인정보의 종류	보존기간
통신비밀보호법 (통신사실확인자료)	로그기록자료, 접속지의 추적자료	3개월
	전기통신일시, 전기통신개시·종료시간, 사용도수, 상대방의 가입자번호, 발신기지국의 위치추적자료	12개월
전자상거래등에서의 소비자보호에 관한 법률 (거래기록)	소비자의 불만 또는 분쟁처리에 관한 기록	3년
	계약 또는 청약철회 등에 관한 기록, 대금 결제 및 재화 등의 공급에 관한 기록	5년
전자금융거래법 (전자금융거래기록)	건당 거래금액 1만원 이하 전자금융거래에 관한 기록, 전자지급수단 이용과 관련된 거래승인에 관한 기록	1년
	전자금융거래 종류 및 금액, 상대방에 관한 정보, 지급인의 출금 동의에 관한 사항, 전자금융거래와 관련한 전자적 장치의 접속기록, 전자금융거래 신청 및 조건의 변경에 관한 사항, 건당 거래금액 1만원 초과 전자금융거래에 관한 기록	5년
신용정보의 이용 및 보호에 관한 법률	신용정보 업무처리에 관한 기록	3년
의료법 (진료에 관한 기록)	처방전	2년
	진단서 등의 부본	3년
	환자 명부, 검사소견기록, 간호기록부, 방사선 사진 및 그 소견서, 조산기록부	5년
	진료기록부, 수술기록	10년
국세기본법	국세 부과 제척기간(조세시효)	10년
	국세징수권 및 국세환급금 소멸시효	5년
상법	보험금액 청구권 소멸시효, 보험료/적립금 반환청구권 소멸시효	2년
	상사채권 소멸시효, 배당금 지급청구권 소멸시효	5년
	사채상환청구권 소멸시효	10년
제조물책임법	손해배상청구권 소멸시효	3년/10년

❍ 이용자의 요청에 따라 기간을 달리 정한 경우

- 이용자의 요청이 있을 경우 예외적으로 1년 이외의 서비스 미이용 기간을 정할 수 있습니다.

- 이용자가 유학, 군입대, 입원, 질병 등으로 장기간 해당 정보통신서비스를 이용할 수 없는 경우, 정보통신서비스 제공자등에게 1년 이외의 서비스 미이용 기간을 요청하여 정하는 것이 가능합니다.

- 1년 이외의 기간으로 정하고자 하는 경우, '이용자의 요청'에 따라 서비스 미이용 기간을 정할 수 있도록 하시기 바랍니다. 예를 들어, 서비스 미이용 기간을 3년으로 정하고자 할 때, 이용자가 이를 선택하여 요청할 수 있는 형태로 제시하는 것이 좋습니다.

(예시①) 개인정보를 파기 또는 분리 저장·관리하여야 하는 서비스 미이용 기간을 [3]년으로 요청합니다.
※ 다만, 별도의 요청이 없을 경우 서비스 미이용 기간은 1년으로 합니다.

(예시②) 개인정보를 파기 또는 분리 저장·관리하여야 하는 서비스 미이용 기간을
2년 [V]
3년 [ ]
회원탈퇴시까지 [ ]
으로 요청합니다.
※ 다만, 별도의 요청이 없을 경우 서비스 미이용 기간은 1년으로 합니다.

다. 정보통신서비스 미이용 판단 기준

❍ 정보통신서비스 이용자(또는 가입자)가 정보통신서비스를 마지막으로 이용한 이후 시행령 제16조제1항에 따른 기간 동안 이용한 기록이 없다면 해당 정보통신서비스 미이용자로 볼 수 있습니다.

- 온라인 서비스의 경우에는 업종별 특성을 고려하여 '서비스 이용기록', '접속 로그' 등을 기준으로 서비스 이용여부를 판단할 수 있으며, 이용자의 이해를 돕기 위해 이용약관 등을 통해 그 적용기준에 대해 명확히 알려주는 것이 바람직합니다.

- 초고속인터넷, 핸드폰 등과 같이 오프라인 서비스 가입 후 웹사이트(온라인) 서비스를 함께 이용하는 온·오프라인 연계 서비스의 경우에는 오프라인에서의 이용도 이용으로 볼 수 있으며, 고객센터 등을 통해 상담문의 등의 기록이 있는 경우에도 이용으로 볼 수 있습니다.

❍ 정보통신서비스제공자등이 광고 문자나 메일을 보낸 기록은 이용기록으로 볼 수 없고, 이용자가 광고 문자나 메일을 단순히 확인하였다는 사실만으로는 ‘이용’으로 볼 수 없습니다.

❍ 기존 가입자의 경우 정보통신서비스 미이용 기간은 시행령 부칙 제1조 및 제2조에 따라 개정 정보통신망법 시행령의 시행일인 2015년 8월 18부터 역산하여 1년이 되는 2014년 8월 18일을 기산점으로 산정합니다.

라. 개인정보 파기 및 분리 저장·관리 방법

❍ 개인정보 파기 방법

- 시행령 제16조제1항에서 정하는 기간 동안 해당 정보통신서비스를 이용하지 않은 이용자의 개인정보는 복구·재생할 수 없는 상태로 파기해야 합니다.

- 종이에 출력된 개인정보나 가입신청서 등 개인정보가 기재된 문서는 분쇄기로 분쇄하거나 소각해야 하고, 컴퓨터 파일 형태로 저장된 개인정보 기록은 재생할 수 없는 기술적 방법(로우레벨포맷 등)으로 삭제해야 합니다.

❍ 개인정보 분리 저장·관리 방법

- 정보통신서비스 제공자등은 장기 미이용자의 개인정보를 보호하기 위해 해당기간 경과 후 즉시 파기하거나 파기에 준하는 조치의 일환

으로 개인정보를 다른 이용자의 개인정보와 분리하여 별도로 분리 저장·관리할 수 있습니다.

- 장기 미이용자의 개인정보는 일반 이용자의 개인정보 DB와 분리하여 별도로 저장·관리하고 일반 직원들의 접근을 제한하는 등 접근 권한을 최소화해야 합니다.

- 별도 저장·관리를 하는 개인정보에 접근통제를 하지 않아 모든 개인정보 취급자가 접근할 수 있도록 운영하는 것은 유효기간제의 입법취지에 반하며, 파기 등 필요한 조치를 취한 것으로 볼 수 없습니다.

- '필요한 조치'로서 별도 저장·관리는 파기에 준하는 조치이므로 물리적으로 DB를 분리하여 저장하는 것이 바람직하나, 테이블 분리 등 논리적으로 분리하는 것도 가능합니다.

- 이용자의 잔여 마일리지, 적립 포인트 등이 남아 있어 이용자의 권리를 보호할 필요가 있고, 향후 재이용의 가능성이 높다고 판단되는 경우에는, 이용자의 재이용 요청이 있는 경우를 대비하여 온라인 이용자의 편의성을 높이기 위한 목적으로 아이디 등 최소한의 연결값을 서비스 중인 DB에 남겨두는 것은 가능합니다.

- 유효기간제의 취지는 1년동안 서비스를 이용하지 않는 이용자의 개인정보를 파기하거나 안전하게 별도 분리 보관하도록 하여 유출 위험 등으로부터 개인정보를 안전하게 보호하기 위한 것이므로, 이용자가 공개를 목적으로 인터넷 상에 게시한 콘텐츠까지 대상에 포함되지는 않습니다. 또한 콘텐츠 작성자 표시 정보와 함께 서비스에 이용 중인 DB에 보관하여 게시글 등이 최초 이용자가 의도한 대로 표시되도록 운영할 수 있습니다.

- 분리 저장·관리되는 개인정보는 재이용하거나 제3자에게 제공할 수 없는 상태임을 전제로 합니다. 다만, 다음의 경우에는 예외로 합니다.

  · 이용자가 정보통신서비스 재이용(계정 활성화)을 요구하는 경우에는 해당 이용자의 개인정보에 접근·이용할 수 있습니다.

  · 정보통신망법(제64조 자료의 제출 등) 또는 형사소송법(제106조 압수, 제109조 수색, 제139조 검증), 통신비밀보호법(제13조 범죄수사를 위한 통신사실 확인자료 제공의 절차, 제13조의2 법원에의 통신사실 확인자료 제공, 제13조의4 국가안보를 위한 통신사실 확인자료 제공의 절차 등) 등과 같이 법률에 특별한 규정이 있는 경우에는 예외로 합니다.

마. 파기 등 조치 대상 개인정보의 범위

❍ 시행령 제16조제2항에서의 파기 등 조치 대상이 되는 개인정보의 범위는 다음과 같습니다.

- 최초 회원가입 또는 회원정보 수정 등의 단계에서 수집·관리되는 개인정보뿐만 아니라 접속 로그(log), 쿠키(cookie), 결제 기록 등 서비스를 이용하는 과정에서 생성되는 정보도 파기 등 필요한 조치의 대상이 되는 개인정보에 포함됩니다.

- 예를 들어 이름, 생년월일, 전자우편, 전화번호, 주소 등 직접 수집하는 인적정보와 서비스 이용 과정에서 생성되어 다른 정보와 쉽게 결합하여 개인 식별이 가능한 경우 해당 정보도 파기 등 조치 대상 개인정보로 볼 수 있습니다.

바. 유효기간 도래 통지 시기 및 방법

❍ 정보통신서비스 제공자등은 서비스 미이용 기간 만료 30일 전까지 전자우편, 서면, 모사전송(팩스), 전화 등의 방법 중 하나를 선택하여 해당 이용자에게 본인의 개인정보가 파기 또는 분리 저장·관리가 되는 사실 및 일시, 개인정보 항목을 통지하여야 합니다.

사. 연락처 부재·변경·오류 등으로 통지가 불가능한 경우

❍ 정보통신서비스 제공자등은 법 제29조 및 시행령 제16조에 따라 개인정보 파기 또는 분리 저장·관리되는 사실을 이용자에게 통지하였으며, 통지의 오배송에 대한 고의·과실이 없음을 입증할 수 있어야 합니다.

- 다만, 신규 회원 가입시 서비스 이용약관 및 개인정보 취급방침 등에 제도의 주요 내용을 공지하고, 기존 이용자에 대해서는 공지사항, 전자우편 등 이용자가 알아볼 수 있는 방법으로 서비스 미이용 기간 만료 후 개인정보가 파기 등의 조치가 취해질 수 있다는 사실 및 정확한 연락처 정보를 제공·수정하도록 적극적으로 알리려는 노력을 해야 할 것입니다.

※ 개정된 본 조항의 시행 시점은 2015.8.18이며, 이 시점으로부터 역산하여 1년간 이용기록이 없는 이용자의 개인정보에 대하여 파기 등 필요한 조치를 취하여야 합니다. 즉, '14.8.18부터 '15.8.17까지 이용기록이 없는 이용자의 개인정보에 대하여 2015.8.18.에 파기 등 필요한 조치를 취하여야 합니다.

9 법정손해배상제 도입

◎ 개정 내용 ◎

개인정보가 분실·도난·누출된 경우 이용자는 손해액을 입증하지 않고 300만원 이하의 범위에서 손해배상을 청구할 수 있는 법정손해배상제가 도입되었습니다. 또한, 이용자가 누출 등의 사실을 안날부터 3년 또는 누출 등이 된 날부터 10년 내에 법정손해배상을 청구할 수 있도록 하는 규정이 신설되었습니다.

◎ 법령 ◎

법률

제32조의2(법정손해배상의 청구) ① 이용자는 다음 각 호의 모두에 해당하는 경우에는 대통령령으로 정하는 기간 내에 정보통신서비스 제공자등에게 제32조에 따른 손해배상을 청구하는 대신 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

1. 정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우
2. 개인정보가 분실·도난·누출된 경우

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

시행령

제18조(법정손해배상의 청구기간) ① 법 제32조의2제1항에 따른 배상은 이용자가 개인정보의 누출등의 사실을 안 날부터 3년 이내에 청구하여야 한다.

② 법 제32조의2제1항에 따른 배상은 개인정보의 누출등이 발생한 날부터 10년이 지나면 청구하지 못한다.

◎ 해설 ◎

❍ 법정손해배상제의 도입으로 이용자는 실제 발생한 손해액을 입증하지 않고 법에서 정하는 범위에서 손해배상을 청구할 수 있습니다.

❍ 법률에서는 손해배상을 청구할 수 있는 금액의 상한을 규정하고 있는 것이며, 손해배상액에 대한 최종 판단은 법원이 하게 됩니다.

❍ 이용자는 개인정보가 분실·도난·누출된 경우에 한해 법정손해배상을 청구할 수 있으며, 누출 등이 발생한 사실을 안날부터 3년, 누출 등이 발생한 날부터 10년 이내에 청구하여야 합니다. 즉, 법정손해배상의 청구기간은 민법 제766조 손해배상청구권의 소멸시효 규정과 동일한 취지의 규정입니다.

※ 이용자는 개정 법률의 시행일인 2014.11.29. 이후 개인정보가 분실·도난·누출된 경우 법정손해배상을 청구할 수 있습니다.

10 과징금 부과 상한액 상향 등

◎ 개정 내용 ◎

위반행위의 구별 없이 과징금 상한을 높이고(관련 매출액의 100분의1 → 관련 매출액의 100분의3), 개인정보 분실 등의 경우 보호조치 위반에 대해 위반행위와 관련한 매출액으로 부과기준을 통일하였습니다. 또한 수탁자가 개인정보보호 규정을 위반한 경우 위탁자에게 과징금을 부과하도록 신설하였고 개인정보 누출과 기술적·관리적 보호조치 위반과의 인과관계 입증 없이 과징금을 부과하도록 하였습니다. 기본과징금 산정 시에는 부과기준율을 매우 중대한 위반행위(0.9%→2.7%), 중대한 위반행위(0.7%→2.1%), 일반 위반행위(0.5%→1.5%) 상향하였습니다. (영 별표8)

◎ 법령 ◎

법률

제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

1. 제22조제1항을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우
2. 제23조제1항을 위반하여 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 경우
3. 제24조를 위반하여 개인정보를 이용한 경우
4. 제24조의2를 위반하여 개인정보를 제3자에게 제공한 경우
5. 제25조제1항을 위반하여 이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 경우

5의2. 제25조제4항에 따른 관리·감독을 소홀히 하여 수탁자가 제4장의 규정을 위반한 경우

6. 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 경우로서 제28조제1항제2호부터 제5호까지의 조치를 하지 아니한 경우
7. 제31조제1항을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 경우

◎ 해설 ◎

❍ 제64조의3 제1항 제6호(이용자의 개인정보를 분실・도난・누출・변조 또는 훼손한 경우로서 제28조 제1항 제2호부터 제5호까지의 조치를 하지 아니한 경우)에 대하여 개정 전 법률에서는 1억원 이

하의 과징금을 부과할 수 있다는 단서가 있었으나 개정 법률에서는 단서를 삭제하여 ‘위반행위와 관련한 매출액’의 100분의3 이하에 해당하는 금액을 과징금으로 부과하게 되었습니다.

- 또한, 개인정보 누출과 기술적·관리적 보호조치 위반과의 인과관계 입증 없이도 과징금 부과가 가능하게 되었습니다.

❍ 정보통신서비스 제공자등이 개인정보 취급위탁을 하는 경우 수탁자에 대한 관리·감독 의무가 있는데, 이를 소홀히 하여 수탁자가 개인정보보호 규정을 위반한 경우 정보통신서비스 제공자등(위탁자)에게 과징금을 부과할 수 있도록 조문을 신설하여 위탁자의 관리·감독책임을 강화하였습니다.

❍ 위반행위 관련 매출액은 위반 행위에 직·간접적으로 영향을 받는 서비스의 연평균 매출액을 의미하는데,

- 해당 정보통신서비스 제공자등의 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액을 말합니다.

- 매출액의 산정시 서비스 범위는 전기통신사업법 제5조를 기준으로 판단하되, 구체적인 판단에 있어서는 다음의 사항을 고려하여야 합니다.

1. 서비스 제공 방식
2. 서비스 가입 방법(서비스 가입시 온라인 가입인지 오프라인 가입인지 여부 및 하나의 사업자가 수개의 웹사이트를 운영하는 경우 독립되어 각각 별개의 가입을 요구하는지 여부 등을 의미한다)
3. 이용약관에서 규정한 서비스의 범위
4. 개인정보 데이터베이스 관리 조직·인력 및 시스템 운영 방식

- 서비스에 대한 매출액은 회계자료를 참고하여 정하되, 이를 통해 위반행위와 관련한 서비스의 매출액을 산정하기 곤란한 경우에는 정보통신서비스 제공자등의 과거 실적, 동종 유사 서비스 제공사업자의 과거 실적, 사업계획, 그 밖에 시장상황 등을 종합적으로 고려하여 매출액을 산정할 수 있습니다.

Ⅲ 개정 정보통신망법 및 시행령 Q&A

1. 필요한 최소한의 개인정보 개념 명확화(법 제23조)

Q **[용어 의미]** 필요한 최소한의 개인정보의 개념을 명확하게 했다고 하나, '해당 서비스', '본질적 기능' 등의 용어를 사용하여 여전히 그 의미를 이해하기 어려운데 어떤 의미인가요?

A

⇨ 해당 서비스는 사업자가 이용자에게 정보통신망을 통해 이용약관 등에 따라 제공하는 개별 서비스를 말하며, 본질적 기능은 사업자가 해당 서비스 제공 과정에서 업무처리를 위해 반드시 필요한 기능을 의미합니다.

이와 관련한 예시 등 자세한 사항은 온라인 개인정보 취급 가이드라인('14.11.12, www.i-privacy.kr/자료실/가이드)을 참고하시기 바랍니다.

2. 개인정보의 취급위탁시 동의 예외 요건 강화(법 제25조제2항)

Q **[마케팅 동의]** 이용자가 마케팅 목적으로 개인정보를 이용하는 것에 대해 동의를 했을 경우 마케팅을 위해 개인정보 취급위탁을 하는 것은 계약 이행에 필요한 사항이므로 개인정보 취급위탁에 대한 별도 동의를 받지 않아도 되는 것 아닌가요?

A

⇨ 마케팅은 정보통신서비스 계약 이행의 본질적인 부분으로 볼 수 없기 때문에 온라인 개인정보 취급 가이드라인에서도 별도 동의를 받도록 안내하고 있으며, 마케팅 목적으로 개인정보를 취급위탁 하는 것은 계약이행에 필요한 것으로 볼 수 없습니다.

또한, 이번 법 개정으로 동의 없이 개인정보 취급위탁을 하려면 이용자 편의 증진 등을 위하여 필요한 경우에 해당하여야 하나, 마케팅 목적으로 개인정보 취급위탁을 하는 것은 이용자 편의 증진과 관련이 없는 것으로 판단됩니다.

3. 영업양수자등의 통지의무 강화(법 제26조제2항)

Q **[영업양수자등 통지의무]** 영업 양도로 인해 개인정보가 이전되는 경우 양도자가 이용자에게 고지를 했다면 양수자는 별도로 고지를 하지 않아도 되는 것 아닌가요?

A

⇨ 정보통신망법의 개정으로 양도자, 양수자 모두 이용자에게 고지해야 합니다. 다만, 고지해야 할 항목에 다소 차이가 있습니다.

양도자는 개인정보를 이전하려는 사실, 양수자의 성명, 주소, 전화번호 및 연락처, 동의 철회 방법과 절차를 고지해야 하며, 양수자는 개인정보를 이전받은 사실, 양수자의 성명, 주소, 전화번호 및 연락처를 고지해야 합니다.

4. 개인정보 취급방침의 전자적 표시의무 폐지(영 제14조제3항)

Q **[전자적 표시 폐지]** 개인정보 취급방침 전자적 표시의무가 폐지된다고 했는데, 이제 개인정보 취급방침을 홈페이지 첫 화면에 게시를 안 해도 되는 것인지요?

A

⇨ 개인정보 취급방침의 전자적 표시*와 인터넷 홈페이지 공개는 전혀 다른 것입니다. 개인정보 취급방침은 정보통신망법 제27조의2에 따라 앞으로도 계속 홈페이지 첫 화면에 공개하여야 합니다.

* 개인정보 취급방침의 전자적 표시 : 개인정보 취급방침에 포함되어야 할 사항을 W3C(World Wide Web Consortium)에서 제정한 P3P(Platform for Privacy Preferences)의 표준 데이타 및 XML 구문 형식에 따라 작성하는 것을 의미

5. 개인정보 누출 통지·신고 기한 명확화 등(법 제27조의3제1항 및 영 제14조의2)

Q **[개인정보 누출 통지·신고]** 개인정보 누출시 정당한 사유 없이 24시간을 경과하여 통지 및 신고를 하면 안된다고 개정되었는데, 정당한 사유에는 어떤 것이 있나요?

A

⇨ 정당한 사유를 명확하게 열거하는 것은 어려우며, 구체적인 상황에 따라 판단이 달라질 수 있습니다. 다만, 다음과 같은 기준에 따라 정당한 사유에 해당할 수 있습니다.

< 이용자에 대한 통지 지연의 정당한 사유(예시) >

· 수사상의 이유 (ex. 경찰이 이용자 통지에 대해 보류를 요청한 경우)
· 물리적·기술적·관리적인 사유로 통지가 불가능한 경우
· 그밖에 단전, 홍수, 폭설 등의 천재지변으로 인해 24시간 내에 통지가 불가능한 경우

< 누출 신고 지연의 정당한 사유(예시) >

· 단전, 홍수, 폭설 등의 천재지변으로 인해 24시간 내에 신고가 불가능한 경우

6. 개인정보의 암호화 대상 개선(영 제15조제4항)

Q **[개인정보 암호화]** 비밀번호는 일방향 암호화 저장하고, 그 밖에 방송통신위원회가 고시하는 정보를 암호화 저장하도록 개정 되었는데, 방송통신위원회 고시는 어떤 것을 의미하며, 어떤 개인정보를 암호화 해야 하나요?

A

⇨ 시행령 제15조제4항제2호에서 방송통신위원회 고시는 "개인정보의 기술적·관리적 보호조치 기준"을 의미합니다.

현행법상 암호화 대상 정보는 바이오정보, 주민등록번호, 신용카드번호, 계좌번호를 암호화 하도록 규정하고 있으나, 시행령 개정에 따라 고시 개정을 추진하고 있으며, 운전면허번호, 외국인등록번호, 여권번호 등 고유식별번호가 추가될 예정입니다.

7. 개인정보 파기의무 및 처벌 강화(법 제29조제1항 및 제73조)

Q **[형사처벌 대상]** 개정 정보통신망법 시행일인 2014.11.29. 이전에 파기했어야 할 개인정보를 보관하고 있다가 시행일 이후에 적발된 경우 형사처벌 대상인가요?

A

⇨ 행위시법주의에 따라 위반행위가 있었던 시점에 시행되고 있는 법률이 적용되는 것이 원칙입니다.

시행일 이전에 파기했어야 할 개인정보를 시행일 이후에도 보관하고 있는 것은 위반상태가 지속되고 있는 것이고, 최초 위반행위는 시행일 이전이나 적발시점까지 위반행위가 있는 것입니다. 따라서, 위반행위시 법률인 개정 정보통신망법에 따라 형사처벌 대상이 됩니다.

다만, 시행일 이전에 개인정보 파기의무를 위반한 사실이 있으나 시행일 이후에는 모두 파기하여 위반행위가 종료된 경우에는 형사처벌 대상에 해당하지 않습니다.

Q **[형사처벌 대상]** 개정된 정보통신망법에 따라 개인정보 파기의무 위반시 형사처벌도 가능하다고 하는데, CEO가 형사처벌 대상인지 아니면 CPO가 형사 처벌 대상인지요?

A

⇨ CPO의 경우 기본적으로 처벌 대상으로 보고 있으며, CEO에 대해서는 구체적인 상황에 따라 판단이 달라질 수 있습니다. 개인정보를 파기하지 않은 사실이 CEO에게 보고되어 해당 사실을 인지하고 있었다면 CPO와 CEO 동시에 형사처벌이 이루어 질수 있습니다.

8. 개인정보 유효기간 단축(영 제16조제1항)

Q **[유효기간제]** 개인정보 유효기간 관련 규정은 시행일이 2014.11.29.이 아니라 2015.8.18.로 되어 있는데, 그 이유는 무엇이며, 실제로 이용자의 개인정보를 파기 등의 조치를 취해야 하는 시점이 언제인가요?

A
⇨ 기존 3년 유효기간제에 따라 파기 등 필요한 조치를 취해야 하는 시점이 2015년 8월 18일이었기 때문에, 사업자의 혼란을 최소화 하기 위해 시행일을 별도 조정한 것입니다.

2015년 8월 18일이 시행일이므로 역산하여 1년이 되는 2014년 8월 18일을 기산점으로 2015년 8월 17일 까지 서비스를 이용하지 않는 이용자의 개인정보에 대해 2015년 8월 18일에 파기 등 필요한 조치를 취하면 됩니다.

Q **[유효기간제]** 개인정보 유효기간제 준수를 위해 사업자는 매일 유효기간이 경과한 이용자의 개인정보를 파기해야 하는지, 아니면 주기적으로 해도 되는지요?

A
⇨ 이용자별로 유효기간 경과시점이 다를 것이므로 매일 확인하여 파기 등 필요한 조치를 하는 것이 원칙입니다. 다만, 현실적으로 매일 확인하여 조치를 취하는 것이 어려울 수 있으므로 유효기간이 도래한 시점부터 영업일 기준 5일 이내에 파기 등 필요한 조치를 취한다면 적법한 것으로 판단할 수 있을 것입니다.

Q **[유효기간제]** 법에서는 유효기간이 1년으로 되어 있지만, 이용자가 유효기간을 별도로 정할 수도 있는데, 그렇다면 사업자는 이용자에게 유효기간을 선택할 수 있는 기능을 의무적으로 제공해야 하나요?

A
⇨ 시행령에서 이용자의 요청에 따라 기간을 달리 정한 경우 유효기간을 달리할 수 있도록 되어 있으므로 사업자가 이용자에게 선택권을 부여하고 이용자 스스로 유효기간을 선택할 수 있도록 하는 것이 바람직하나 의무사항은 아닙니다.

Q **[유효기간제]** 개인정보 유효기간 관련 '이용'의 의미는 로그인 기록을 말하는 것인지, 미이용 기간 1년의 기산일은 언제를 말하는 것인지요?

A

⇨ 이용은 로그인 기록 등으로 단순하게 판단할 수는 없으며, 전화상담 또는 고객센터 문의 등 오프라인 이용도 이용에 해당할 수 있습니다. 또한, 레터링 서비스와 같이 어떤 정보를 주기적으로 발송하는 것을 서비스 계약의 주요내용으로 하는 경우에는 해당 레터를 이용자가 계속 수신하고 있다면 이용을 하는 것으로 볼 수 있습니다.

그러나, 사업자가 마케팅 동의를 받아 이용자에게 광고성 메일이나 안내 메일을 발송하고 이용자가 이를 수신하였다 하더라도 이는 이용으로 볼 수 없습니다.

미이용 기간의 기산일은 이용자의 최종 이용일입니다.

Q **[유효기간제]** 사용자가 계정 제재를 당해 계정이용이 제한되는 경우, 그 기간을 이용하지 않은 기간에 포함시킬 수 있나요?

A

⇨ 유효기간제의 기산일은 이용자가 최종 이용한 시점이 기준이며, 사업자 내부정책에 따라 이용 제한을 하는 경우까지 고려하여 기산일을 달리 정할 수는 없습니다.

Q **[유효기간제]** 이용자로부터 영리목적의 광고성 정보 전송에 대한 수신동의를 받았는데, 유효기간이 경과하여 이용자의 개인정보를 별도 분리·저장한 경우 정보통신망법 제50조에 따른 영리목적의 광고성 정보 전송에 대한 2년 주기의 수신동의 여부를 확인해야 하나요?

A

⇨ 유효기간이 경과한 이용자의 개인정보를 별도 분리·저장한 경우 해당 이용자의 개인정보는 이용자의 요청이 없는 한 이용할 수 없으므로, 영리목적의 광고성 정보를 전송해서는 안됩니다.

영리목적의 광고성 정보 전송에 대한 수신동의 여부를 2년마다 확인하도록 하는 취지는 최초에 수신동의를 했다 하더라도 앞으로도 계속해서 수신할 것인지 선택권을 주고자 함입니다. 따라서, 영리목적의 광고성 정보를 전송해서는 안되는 이용자에게 수신동의 여부를 확인할 필요는 없을 것으로 판단됩니다.

Q **[유효기간제]** 2015.8.18이후 개인정보 보관 유효기간 단축 관련하여 1년간 서비스 미이용시 아래 법률에 해당 되는 개인 정보들은 어떻게 해야 하나요?

상업장부와 고객정보를 포함한 영업에 관한 중요서류: 10년 (상법 제33조)
고객정보를 포함한 전표 또는 이와 유사한 서류: 5년 (상법 제33조)
계약 또는 청약철회 등에 관한 기록: 5년 (전자상거래법 제6조제3항 및 동법 시행령 제6조제1항)
대금결제 및 재화 등의 공급에 관한 기록: 5년 (전자상거래법 제6조제3항 및 동법 시행령 제6조제1항)
소비자의 불만 또는 분쟁처리에 관한 기록: 3년 (전자상거래법 제6조제3항 및 동법 시행령 제6조제1항)

A

⇨ 정보통신망법 시행령 제16조제1항 각 호에서는 유효기간 1년에 대한 예외를 규정하고 있습니다.

1. 다른 법령에서 별도의 기간을 정하고 있는 경우: 해당 법령에서 정한 기간
2. 이용자의 요청에 따라 기간을 달리 정한 경우: 달리 정한 기간

따라서, 위와 같이 개별 법령에서 개인정보 보존기간을 정하고 있는 경우에는 해당 법령에서 정한 기간 동안 보관이 가능합니다. 다만, 해당 법령에 따라 일정기간 보관이 가능한 것일 뿐 사업자가 그 기간 동안 이용해도 된다는 의미가 아니므로 별도 보관해야 합니다.

Q **[유효기간제]** 형사소송법, 통신비밀보호법 등에 따른 압수수색 등 개인정보 제공 요청이 있는 경우 유효기간제에 따라 별도 분리 보관된 회원에 대한 정보 제공이 가능한지요?

A

⇨ 유효기간이 경과하여 별도 분리 보관한 이용자의 개인정보는 이용하거나 제3자에게 제공할 수 없는 것이 원칙이지만, 형사소송법, 통신비밀보호법 등 법령에 근거하여 수사기관이 제공을 요청한 경우에는 제공할 수 있습니다.

Q **[유효기간제]** 이용자와의 별도 계약(약관 포함)으로 유효기간을 설정하는 것이 정보통신망법 시행령 제16조제1항제2호의 "이용자의 요청에 따라 기간을 달리 정한 경우"에 해당하나요?

A

⇨ 약관으로 사업자가 개인정보 유효기간을 정하여 이용자의 동의를 받은 경우는 정보통신망법 시행령 제16조제1항제2호의 '이용자의 요청에 따라 기간을 달리 정한 경우'에 해당하지 않습니다. '이용자의 요청에 따라 기간을 달리 정한 경우'에 해당하려면 이용자가 직접 기간을 요청하거나 선택할 수 있어야 합니다.

Q **[유효기간제]** 오프라인으로만 가입되어 있는 회원(온라인 미가입 회원)에 대하여도 유효기간제가 적용 되나요?

A

⇨ 개인정보 유효기간제 적용 여부는 해당 사업자가 정보통신망법을 적용받는 정보통신서비스 제공자인지 여부에 따라 결정됩니다. 이용자의 개인정보를 온라인으로 수집했는지 오프라인으로 수집했는지 여부는 관계가 없습니다.

오프라인으로만 사업을 운영하는 사업자로서 정보통신서비스 제공자에 해당하지 않는다면, 개인정보 보호법의 적용을 받으므로 유효기간제 적용 대상이 아닙니다.

Q **[유효기간제 사전통지]** 개인정보 수집시 이메일, 연락처 등을 수집하지 않아 이용자에게 통지할 수단이 없을 경우 어떻게 해야 하나요?

A

⇨ 이용자에게 개별 통지는 불가능하므로 서비스 미이용 기간 만료 후 개인정보가 파기 등의 조치가 취해질 수 있다는 사실을 서비스 이용약관 및 개인정보 취급방침 등을 통해 이용자에게 알리면 될 것으로 판단됩니다.

Q **[유효기간제]** 유효기간이 경과한 이용자의 정보는 파기하거나 DB를 별도 분리보관 해야 한다고 하는데 분리보관을 하게 되면 계속 보유가 가능한가요?

A

⇨ 별도 분리보관을 하게 되더라도 개인정보 수집·이용시 명시한 보유기간이 종료되거나 이용자의 동의철회, 회원탈퇴 등 파기사유가 발생하면 지체없이 파기해야 합니다.

Q **[유효기간제]** 1년 동안 이용내역이 없는 이용자의 정보는 별도 보관 등의 조치를 취해야 하는데 별도 보관한 이용자를 대상으로도 정보통신망법 제30조의2에 따른 이용내역을 통지해야 하나요?

A

⇨ 이용내역 통지제는 이용자의 개인정보를 이용한 내역을 이용자에게 알려주기 위한 제도인데, 1년 동안 서비스를 이용하지 않은 이용자에게 이용내역 통지는 필요하지 않을 것으로 판단됩니다.

Q **[유효기간제]** 개인정보의 유효기간제에 따라 1년동안 이용하지 않는 이용자의 개인정보는 별도로 분리 보관하여야 합니다. 분리 보관의 대상에 이용자가 공개를 목적으로 작성한 게시글, 댓글 등의 콘텐츠 정보와 작성자 정보(아이디, 별명 등)도 포함되나요?

A

⇨ 유효기간제의 취지는 1년동안 서비스를 이용하지 않는 이용자의 개인정보를 파기하거나 안전하게 별도 분리 보관하도록 하여 유출 위험 등으로부터 개인정보를 안전하게 보호하기 위함입니다.

따라서, 이용자가 공개를 목적으로 인터넷 상에 게시한 콘텐츠까지 포함하지는 않습니다. 또한 콘텐츠 작성자 표시 정보와 함께 서비스에 이용 중인 DB에 보관하여 게시글 등이 최초 이용자가 의도한 대로 표시되도록 운영할 수 있습니다.

게시글 등 이용자가 공개를 목적으로 작성한 콘텐츠와 관련한 사항은 서비스 이용약관 등에 명시하여 관련 절차에 따라 삭제 등의 절차를 운영하는 것이 바람직합니다.

Q **[유효기간제]** 이용자가 유효기간 경과 후 서비스의 재이용을 원할 경우를 대비하여 유효기간 경과에 따라 이용자의 개인정보를 별도 DB에 보관 하더라도 이용자의 재이용 편의성 제공을 위해 최소한의 정보를 서비스 DB에 보유하여도 되나요?

A

⇨ 이용자가 1년 동안 서비스를 이용하지 않은 경우에는 이용자의 모든 개인정보를 파기하는 것이 원칙입니다. 다만, 이용자의 잔여 마일리지, 적립 포인트 등이 남아 있어 이용자의 권리를 보호할 필요가 있고, 향후 재이용 가능성이 높다고 판단되는 경우에는 별도 분리 보관할 수 있습니다.

또한, 추후에 이용자의 재이용 요청이 있는 경우를 대비, 온라인 이용자의 편의성을 높이기 위하여 아이디 등 최소한의 연결값을 서비스 중인 DB에 남겨두는 것은 가능하다고 판단됩니다.

Q **[유효기간제]** 1년 동안 서비스 이용기록이 없는 회원의 개인정보는 반드시 파기해야만 하나요?

A

⇨ 파기할지 여부는 사업자의 환경을 고려하여 판단할 수 있습니다. 1년 동안 서비스 이용기록이 없고 향후에도 이용 가능성이 없다고 판단되는 경우에는 파기하여야 합니다.

다만, 잔여 마일리지, 포인트 등이 남아 있어 이용자의 권리를 보호할 필요가 있고, 향후 이용 가능성이 있다고 판단되는 경우에는 별도 분리 보관하였다가 추후에 이용자의 요청이 있는 경우 서비스에 다시 이용할 수 있습니다. 또한, 이용자의 요청에 따라 별도의 기간을 정한 경우에는 별도 분리 보관없이 그 기간 동안 서비스에 이용이 가능합니다.

Q **[유효기간제]** 1년간 서비스를 이용하지 않은 이용자의 개인정보를 파기 외에 별도 저장 및 보관이 가능한데 반드시 물리적 분리만 허용 되나요?

A

⇨ 법 해석상 별도 저장·관리는 파기에 준하는 조치이므로 물리적 분리를 하는 것이 바람직하나, 논리적 분리(테이블 분리 등)도 허용됩니다.
논리적 분리를 하는 경우 유효기간제의 입법취지에 맞게 접근 통제 및 외부해킹방지 등 필요한 보호조치는 반드시 해야 할 것으로 판단됩니다.

9. 과징금 부과 상한액 상향(법 제64조의3제1항)

Q **[과징금]** 위반행위와 관련한 매출액의 100분의 3까지 과징금 부과가 가능하다고 하는데 위반행위와 관련된 매출액의 범위를 어떻게 산정하나요?

A

⇨ 위반 행위 관련 매출액은 위반 행위에 직·간접적으로 영향을 받는 서비스의 연평균 매출액을 의미하는데, 해당 정보통신서비스 제공자등의 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액을 말합니다.

매출액의 산정시 서비스 범위는 개인정보의 수집·이용 동의 시 목적과 서비스 이용 범위 그리고 이용약관의 서비스 이용 목적 등을 보고 종합적으로 판단하게 됩니다.