

# [데이터 경제 시대의 도래, 기업이 대비해야 할 주요 법안서]

## 8차시. 개인정보의 파기

학습목표
<ul style="list-style-type: none"><li>▪ 학습내용: 해당 차시에서 학습할 학습주제(목차)를 제시해 주세요.</li><li>▪ 학습목표: 해당 차시 학습을 통해 <u>학습자들이 달성해야 할 목표</u>를 학습내용과 연계하여 작성해 주세요.</li></ul>

### ▶ 학습내용

1. 개인정보파기의 시기와 방법
2. 개인정보파일별 보유기간
3. 정보통신사업자에 대한 개인정보파기의 특례
4. 개인정보 파기의무 위반시 벌칙내용
5. 개인정보 파기와 관련된 실전 해석

### ▶ 학습목표

1. 개인정보파기의 시기와 방법을 설명할 수 있다.
2. 주요 개인정보파일의 보유기간을 설명할 수 있다.
3. 정보통신사업자에 대한 개인정보파기의 특례를 설명할 수 있다.
4. 개인정보 파기의무 위반시 벌칙내용을 설명할 수 있다.

학습내용
<ul style="list-style-type: none"> <li>▪ 학습내용의 위계 파악을 위해 일관성 있는 번호 체계로 작성해 주세요.</li> </ul>

## I. 의의

### 1. 개인정보 파기의 중요성 대두

개인정보는 정보주체의 사생활과 관련된 매우 중요한 정보이므로 설령 개인정보 수집 및 이용 등에 관하여 정보주체의 사전동의를 받았다 하더라도, 개인정보의 수집 및 이용 목적이 달성된 경우에는 즉시 파기되어야 한다. 개인정보를 통한 활용가치가 오늘날 더더욱 커짐에 따라 개인정보는 항상 유출과 남용의 위험이 있다. 실제로 2014년 1월에 발생한 신용카드 3사(KB카드 5300만건, 롯데카드 2600만건, NH카드 2500만건)의 안전하리라고 믿었던 금융회사에서 발생한 대규모 개인정보의 유출사고를 통해서 그 피해는 비단 성인 뿐만 아니라 미성년자까지 포함한 경제활동인구의 대다수가 입었던 피해로 기억되면서 전국민을 불안에 빠지게 하였다. 이로부터 개인정보 ‘파기’에 대한 중요성이 크게 대두되기 시작하였다.

이처럼 개인정보는 다양한 목적(분쟁, 신분 및 재산 증명, 세금부과, 사실확인 등)을 위해 일정기간 동안 보존되어야 하므로 개인정보 파기는 예외가 존재한다. 따라서 개인정보를 보유한 개인정보처리자는 물론, 자신의 권리(개인정보결정권)에 대한 보호를 위해 정보주체도 개인정보파기의 원칙과 예외, 그리고 그 방법에 대해 인지를 하고 있어야 한다.

### 2. 개인정보 파기 관련 법규

개인정보의 파기와 관련한 법규로는 개인정보 보호법 뿐만 아니라, 동법 시행령 그리고 표준지침과 고시에 의해서도 이러한 개인정보 파기를 엄격히 규제하고 있다. 개인정보 파기와 관련한 일반적인 내용에 대해서는 개인정보 보호법 제21조에서, 구체적인 파기방법에 대해서는 동법 시행령 제16조에서 규정하고 있다. 뿐만 아니라 개인정보의 보유기간이 경과하거나 처리목적이 달성하는 등의 사유가 있는 경우, 그리고 시행령에 따른 ‘복원이 불가능한 방법’ 등에 대해서는 표준 개인정보 보호지침 제10조와 제11조에서 상세히 규정하고 있다. 나아가 파기의 구체적인 방법에 대해서는 개인정보 안전성 확보조치 기준 제13조에서 구체적으로 그 방법을 적시하고 있다.

## II. 파기의 내용 및 의무

### 1. 파기의 내용

파기란 복원이 불가능한 방법으로 영구 삭제, 파쇄, 소각하는 등 복구 또는 재생되지 않도록 하는 일체의 행위를 말한다. 따라서 개인정보의 “파기”란 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때 지체 없이 그 개인정보를 복원이 불가능한 방법으로 영구 삭제, 파쇄 또는 소각하여 복구 또는 재생되지 아니하도록 조치하는 것을 말한다.<sup>1)</sup> 개인정보의 수집 및 이용이 제한된 범위에서 엄격한 조건아래 이뤄지고 있으므로 개인정보 처리에 대한 목적이 달성되었다면 오남용에 대한 우려를 불식시키기 위해 원칙적으로

1) 한편 신용정보법에서는 개인신용정보의 파기 대신 폐기에 관한 규정을 두고 있다. 신용정보법 제20조, 제21조 참조.

파기되어야 한다.

다만 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우도 있을 수 있으므로, 해당 법령에 따른 기간 동안 보존하여야 하고, 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존하여야 한다.

## 2. 파기의무와 개념정의

개인정보는 정보주체의 프라이버시와 매우 긴밀하게 관련되어 있으므로 개인정보 보호를 위해서는 개인정보의 수집과 이용을 엄격히 제한하는 것만큼이나 개인정보를 보유하고 파기하는 것 또한 엄격히 통제하여야 한다. 이에 따라 개인정보를 보유할 목적이 달성된 경우, 자칫 보유상태에 있다가는 고의 및 과실로 유출되어 오·남용될 가능성이 크므로 목적달성 즉시 파기하도록 하여 안전을 기해야 한다. 이에 따라 「개인정보 보호법」에서는 개인정보의 보유기간 경과, 처리목적 달성 등으로 개인정보가 불필요하게 되면 개인정보처리자는 지체없이 그 개인정보를 파기할 것을 의무화하고 있다(법 제21조 제1항).

이때의 파기는 개인정보가 복구 또는 재생되지 않도록 하여야 하는 것을 의미하는데(개인정보보호법 제21조 제2항), 1. 전자적 파일형태인 경우에는 복원이 불가능한 방법으로 영구삭제하고, 2. 그 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우에는 파쇄 또는 소각하는 방법으로 파기하여야 한다(시행령 제16조 제1항). 전자적 파일형태에서 ‘복원이 불가능한 방법’이란, 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다(표준지침 제10조 제2항).

## 3. 원칙: 즉시파기

개인정보 파기의 원칙은 즉시파기이다. 즉 개인정보처리자는 개인정보의 보유기간이 경과하거나, 개인정보의 처리 목적을 달성하는 등 개인정보를 더 이상 보유할 필요가 없을 때에는 해당 개인정보를 지체없이 즉시 파기하여야 한다(개인정보보호법 제21조 제1항 본문). 이처럼 개인정보의 처리목적 달성시 즉시파기를 원칙으로 하는 이유는 개인정보 활용가능성이 커짐에 따라 목적달성후 파기하지 않고 지속적으로 보유하게 되면 일차적으로는 개인정보처리 내부자로부터 손쉽게 개인정보 처리 목적을 넘어서 활용할 가능성이 높고, 이차적으로는 관리부실에 따른 개인정보유출은 물론이고 제3자의 해킹 등을 통해 보안이 뚫릴 위험성이 매우 높기 때문에 사전에 개인정보를 파기함으로써 이러한 가능성을 차단할 필요가 크기 때문이다.

## 4. 즉시파기원칙의 예외

개인정보 이용의 목적달성시 개인정보는 즉시파기함이 원칙이므로 인터넷사이트 회원가입시 활용되었던 개인정보는 회원탈퇴시 즉시 파기되어야 한다. 그러나 문제는 항상 원칙에는 예외에 따르기 마련이고 이러한 즉시파기원칙도 개인정보를 일정기간 동안 보유하도록 하고 있는 다른 법령을 통해서 예외가 많이 허용되어 있다는 점에서 우려의 목소리가 큰 상황이다. 실제로 개인정보보호법 제21조 제1항 단서에서도 ‘다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.’고 규정함으로써 즉시파기원칙의 예외를 법적으로 허용하고 있는 상황이다. 대표적으로는 상법, 전자상거래 등에서의 소비자 보호에 관한 법률, 전자금융거래법 등에서 일정기간 동안 개인정보를 보유하도록 의무화하고 있는 실정이다. 이에 대한 자세한

내용은 후술하기로 한다.

### III. 파기방법 및 절차

#### 1. 파기의 시기

개인정보처리자가 개인정보를 파기해야 하는 시기는 해당 개인정보가 불필요하게 되었을 때 지체없이 바로 파기하여야 한다(법 제21조 제1항). 개인정보가 불필요하게 되는 사유란 보유기간이 경과하였거나, 개인정보의 처리 목적을 달성한 경우가 대표적인 경우이며, 그 외에도 개인정보처리자의 사업이 종료되었거나, 정보주체의 동의철회나 개인정보 삭제 또는 파기 요청 등이 있는 경우도 개인정보를 파기해야 하는 사유가 된다. 이때 ‘지체없이’의 기일이 어느 정도인지 문제되는데, 표준지침 제10조 제1항에 따르면 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하도록 구체적으로 적시하고 있다.

#### 2. 파기의 방법

한편 개인정보를 파기할 때에는 복원 또는 재생할 수 없도록 파기함이 원칙이다. 그리고 구체적인 파기방법은 개인정보를 보존하는 매체의 특성에 따라 파기방법도 다양할 수 밖에 없다. 개인정보보호법 시행령 제16조 제1항에서는 보존매체에 따른 개인정보의 파기방법에 대해 크게 두가지로 제시하고 있는데, 바로 전자적 파일 형태의 경우와 그 외의 매체로 구분하여 파기방법을 제시하고 있다. 즉 첫째는 전자적 파일 형태인 경우에는 복원이 불가능한 방법으로 영구삭제하도록 하고 있다. 이러한 구체적 예로는 공장초기화 포맷을 하거나, 일반 포맷을 한 뒤 불필요한 정보를 여러 번 덮어쓰워서 재생할 수 없도록 하는 조치를 말한다. 이 외에도 물리적인 힘으로 디스크를 파쇄하거나 자기장치를 이용해 강한 자기장으로 데이터를 삭제하는 방법도 사용된다. 다만 이러한 방법은 디스크를 재사용할 수 없다는 점이 단점으로 꼽힌다. 따라서 영구삭제 소프트웨어를 이용해 여러번 반복해 덮어쓰는 방법이 추천되고 있다.

시행령에서 제시하고 있는 두 번째의 파기방법으로는 위에서 살펴본 전자적 파일 외의 기록물, 인쇄물, 서면, 그밖의 기록매체에 있어서의 파쇄 또는 소각을 명문화하고 있다. 대표적으로는 개인정보가 기재된 문서의 경우 문서세단기로 파쇄하거나 소각시설을 이용해 소각하는 것을 든다.

이러한 개인정보보호법 시행령 외에도 구체적인 파기방법에 대해서는 ‘개인정보보호위원회’에 위임하여 제정한 행정규칙인 「개인정보의 안전성 확보조치 기준」 제13조에서 상세히 적시하고 있다. 즉 1. 완전파괴(소각·파쇄 등), 2. 전용 소자장비를 이용한 삭제, 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행 중에서 하나의 조치를 선택하도록 하고 있다(제1항). 또한 개인정보 전체가 아닌 일부만을 파기하는 경우에 있어서 위의 방법으로 파기하는 것이 어려운 때에는, 첫째, 전자적 파일 형태의 경우에는 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독여야 하고, 둘째, 그 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우에는 해당 부분을 마스킹, 천공 등을 하여 삭제하도록 규정하고 있다(제2항)

나아가 파기방법 및 절차에 대하여 표준지침 제10조에서도 규정하고 있다. 즉 개인정보처리자는 개인정보의 보유기간이 경과하거나 개인정보의 처리목적을 달성하였거나, 해당서비스가 폐지되었거나, 사업이 종료되는 등 그 개인정보가 불필요하게 되었을 때에는, 정당한 사유가

없는 한, 5일 이내에 개인정보를 파기하도록 지침을 마련하였다.

### 3. 파기의 절차

한편 개인정보의 파기는 원칙적으로 개별 개인정보 단위로 이루어져야 한다. 만일 전체 개인정보파일 단위로 파기가 이뤄지게 되면, 개인정보의 처리목적 달성이거나 개인정보의 보유 및 이용기간의 종료 시점이 물리적으로 늦춰질 가능성이 높으므로 그만큼 파기의 시점이 지연될 위험이 크다. 문제는 전자파일의 경우에는 비교적 개인정보 파기가 손쉬우나, 그 밖의 대량문서, 종이문서철 등으로 개인정보가 보관될 경우에는 설령 개인정보의 처리목적이 달성되었다 하더라도, 개별 개인정보를 선택적으로 파기하는 것이 매우 어렵다. 따라서 개인정보 파기가 원활히 이루어지도록 문서로 개인정보가 보관되어 있는 경우에는 단위별(기간별, 개인별, 개인정보유형별, 개인정보 수집 목적별, 이용별 등)로 별도의 점검을 하고 단위별로 파기 가능하도록 하는 조치를 마련해두어야 한다.

나아가 개인정보를 파기할 때에는 파기에 관한 사항에 대해 개인정보처리자는 기록 및 관리를 하여야 한다(표준지침 제10조 제3항). 또한 개인정보 보호책임자는 처리목적이 달성되거나 보유기간이 지난 개인정보에 있어서는 본인의 책임 하에 개인정보 파기를 시행하여야 하며, 또한 파기의 결과에 대해서도 확인하여야 한다(개인정보보호법 시행령 제32조 제1항 제3호 및 표준지침 제10조 제4항).

## IV. 파기의무의 예외 (법 제21조 제1항 단서)

### 1. 즉시파기의 구체적 예외사유

개인정보처리자는 개인정보 보유기간이 경과하거나, 개인정보의 처리목적달성 등 개인정보가 불필요하게 되었을 때에도, ‘다른 법령에 따라 보존해야 하는 경우’에는 예외적으로 개인정보를 파기하지 않고 보존해야 한다(법 제21조 제1항 단서). 다른 법령에 따라 개인정보를 보존해야 하는 경우에는 개인정보처리자의 개인정보 처리방침에 그 보존하는 법적 근거 및 보존하는 개인정보 항목을 명확히 표시하여야 한다(법 제30조 제1항 제3호의 2).

### 2. 법령상 보관 의무있는 개인정보의 보존방법 (법 제21조 제3항)

법 제21조 제1항 단서에 따라 법령상 파기하지 않고 보존하여야 하는 개인정보의 경우, 물리적 또는 기술적 방법으로 해당 개인정보 또는 파일을 다른 개인정보와 분리해서 저장·관리하여야 한다(법 제21조 제3항 및 표준지침 제11조 제1항). 이는 파기되지 않은 개인정보가 기존의 개인정보와 혼재되어 있게 되면, 수집시의 개인정보의 목적 외 이용, 유출, 오남용의 위험이 커지므로 이를 방지할 필요가 위함이다. 따라서 미파기의 보관이 필요한 개인정보는 필요최소한으로 그쳐야 한다. 이에 따라 미파기 개인정보는 다른 법령에서 보존하도록 한 목적 범위 내에서만 저장·관리한다는 점을 개인정보 처리방침 등을 통하여 정보주체가 알 수 있도록 하고 있다(표준지침 제11조 제2항)

### 3. 정보통신서비스제공자 등의 파기에 대한 특례 (법 제39조의6 제1항)

개인정보 파기와 관련해 정보통신서비스 제공자에 대해서는 특례가 있다. 즉 정보통신서비

스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위해, 정보통신서비스 제공자 등은 대통령령에서 정하고 있는 개인정보 파기 등의 필요한 조치를 취하여야 한다(법 제39조의6 제1항). 이에 따라 시행령에서는 정보통신서비스 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 않는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하도록 규정하였다(시행령 제48조의5 제1항). 이 기간에 대하여 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우에는 이에 따르도록 하고 있다(법 제39조의6 제1항 단서).

정보통신서비스 제공자 등은 개인정보를 파기하지 않고 별도로 저장·관리하는 경우에는 이 법 또는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 해당 개인정보를 이용하거나 제3자에게 제공하여서는 안된다(시행령 제48조의5 제2항). 또한 정보통신서비스 제공자 등은 정보통신서비스를 이용하지 않은 1년의 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(법 제39조의6 제2항). 이때 대통령령으로 정하는 사항이란 1. 개인정보를 파기하는 경우: 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목, 2. 다른 이용자의 개인정보와 분리하여 개인정보를 저장·관리하는 경우: 개인정보가 분리되어 저장·관리되는 사실, 기간 만료일 및 분리·저장되어 관리되는 개인정보의 항목을 말한다(법 제39조의6 제2항). 그리고 전자우편 등 대통령령으로 정하는 방법은 서면 등의 방법을 말한다(시행령 제48조의5 제4항).

#### 4. 벌칙

먼저 정보통신서비스 제공자 등이 법 제21조 제1항을 위반하여 개인정보를 파기하지 아니한 경우에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처해지며(제73조 제1의2호), 개인정보 처리자가 제21조 제1항(제39조의14 준용 포함)을 위반하여 개인정보 파기 등의 필요한 조치를 취하지 아니한 경우 3천만원 이하의 과태료가 부과된다. 그리고 제21조 제3항을 위반하여 개인정보를 분리하여 저장·관리하지 않은 경우에도 1천만원 이하의 과태료가 부과된다(제74조 제4항 제1호).

#### V. 실무적용 예2)

개인정보 파기와 관련하여, 앞서 살펴본 개인정보의 보유기간은 개인정보 파일별로 매우 다양하다. 따라서 실제 개인정보처리자는 보유하고 있는 개인정보 파일이 어디에 해당하는지 구체적으로 판단하기에는 쉽지가 않다. 이에 따라 개인정보보호위원회 소속의 ‘개인정보 법령해석 지원센터’에서는 공공기관 직원의 개인정보 보호법 해석능력 향상을 위해 ‘사례 중심 개인정보보호 법령 해석 실무 교재’를 2021년 12월에 출간하였다.

##### [Q] 회원 개인정보 파기시 연계 회원번호도 파기해야 하는지? (표준 해석례 40)

회원관리 시스템에서 회원 탈퇴 시, 이름, 연락처, 주소 등 개인을 식별하는 정보는 모두 지체 없이 파기합니다. 이때, 생성정보였던, 회원번호 000001도 함께 파기하여야 하는 것일까요? 회원번호 신규 생성 등을 위하여, 회원번호만 따로 순차적으로 관리하려 합니다.

▶ [A] 개인을 식별할 수 없는 숫자는 개인정보가 아니므로 파기 불필요

- 「개인정보 보호법」 제21조 제1항에 따라 개인정보처리자는 다른 법령에 따라 보존하여야 하는 경우 이외에는 보유기간이 경과하거나 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때 지체 없이 그 개인정보를 파기하여야 함
- 따라서 개인정보의 처리 목적이 달성된 경우 개인을 식별할 수 있는 정보(이름, 연락처, 주소 등)는 모두 지체 없이 파기해야 함
- 다만, 법 제58조의2에 따라 이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니함
- 따라서 관련정보가 모두 파기되어 연계 생성된 회원번호를 더 이상 누구의 개인정보인지 알아볼 수 없다면 이는 익명 정보로서 파기하지 않아도 됨

[Q] 법정 보존기간이 지난 개인정보를 연장하여 보존해도 되는지? (표준 해석례 42)

전자상거래법 시행령 제6조에 따라 대금결제 및 재화등의 공급에 관한 기록: 5년 등 개인정보 보존기간을 정하고 관리하고 있습니다. 회원이 결제와 관련하여, 7년전 기록에 대한 조회를 요청하는 경우가 있는데, 위 보존기간 이상 개인정보를 보존해도 되는지요?

▶ [A] 고객에게 연장보존에 대한 동의를 받으면 연장하여 보존할 수 있음

- 「개인정보 보호법」 제21조 제1항에 따라 개인정보처리자는 다른 법령에 따라 보존하여야 하는 경우 이외에는 보유기간이 경과하거나 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때 지체 없이 그 개인정보를 파기하여야 함
- 법령에서 보존기간을 별도로 정한 경우 보존기간이 경과되면 지체없이 개인정보를 파기해야 하나, 법 제15조 제2항에서 정한 개인정보의 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 고객에게 알리고 새로 동의를 받으면 연장하여 보존할 수 있음

[Q] 키즈카페는 CCTV 영상을 며칠간 보관해야 하나요? (표준 해석례 62)

찾아보니 일반 상가 또는 가게의 CCTV는 최대 30일까지 보관가능이라고 되어 있고, 유치원 어린이집 같은 경우 60일로 되어 있던데, 키즈카페(어린이 놀이카페) 같은 경우에는 CCTV가 최대 며칠까지 법적으로 보관 가능한가요?

▶ [A] 보유목적 달성을 위한 최소한의 기간동안 보관하되, 보유기간 산정이 어려운 경우 30일 이내 보관함

- 「개인정보 보호법」 제25조 제7항 및 시행령 제25조에 따라 영상정보처리기관운영자는 영상정보 처리기기의 설치근거, 촬영기간, 보관기간 등을 내용으로 하는 영상정보처리기기 운영·관리 방침을 마련하여야 하며, 이때 보관기간은 보유목적의 달성을 위한 최소한의 기간으로 설정하면 됨
- 표준개인정보보호지침 제41조 제2항에 따라 보유목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 할 수 있음
- 한편, 「영유아 보육법」 제15조의4 제3항에 어린이집을 설치·운영하는 자는 CCTV에 기록된 영상정보를 60일 이상 보관하도록 하고 있는바, 이와 같이 다른 법령에서 영상정보의 보관기간이 특별히 규정되어 있는 경우에는 그에 따라야 함