
개인정보 최소수집·보관을 위한

온라인 개인정보 취급 가이드라인(안)

2014. 11.



[순 서]

① 필요 최소한의 개인정보 수집 기준	1
1. 기본 방향	1
2. 해당 서비스의 단계별 수집 기준	4
② 단계별 개인정보 파기 기준	8
1. 개인정보 수집 단계	8
2. 서비스 이용·보관 단계	10
3. 제공 단계	11
4. 파기 단계	12
③ 이해하기 쉬운 동의서 작성 기준	14
1. 동의를 받는 방법	14
2. 동의를 받는 내용	17
☞ 참고 ① 해당 서비스의 본질적 기능과 필수동의 항목(예시)	18
② 법정 수집 의무항목 및 보유기간(예시)	19
③ 동의 사례(예시)	20

〈 기 본 방 향 〉

- ◇ 사업자의 개인정보 **최소 수집·이용 문화 정착**을 위하여 개인정보의 단계별 기준 및 동의절차 기준을 제시
- ◇ ① 사업자가 수집하는 개인정보를 **최소한**으로 줄이고, ② 단계별 불필요한 개인정보는 지체없이 **파기**하도록 하며, ③ **동의서 양식** 등을 이용자가 이해하기 쉽게 작성하도록 기준을 마련

① 필요 최소한의 개인정보 수집 기준

- 필수동의 항목의 범위를 최소화하고, 선택동의 항목에 대한 이용자의 실질적 동의권을 보장
- 필요한 시점에 수집하도록 하여 불필요한 개인정보 수집 제한

② 단계별 개인정보의 파기 기준

- (수집·보유 단계) 수집·이용 목적, 보유기간 등을 명확히 하고, 개인정보 파기 사유 발생시 “지체없이” 파기
- (제공 단계) 서비스와 무관한 제3자 제공을 원칙적으로 제한하고, 제공한 경우 파기확인 등 조치사항을 계약서에 반영
- (파기 단계) 재생할 수 없는 파기방법의 기준을 제시

③ 이해하기 쉬운 동의서 작성 기준

- “법정 고지사항”만을 간결하게 고지하고, “쉬운 용어”, “그림, 표 활용” 등을 사용하여 동의서를 읽기 쉽게 개선
- 필수 동의사항과 그 외 선택 동의사항을 구분하여 동의내용을 한눈에 알아 볼 수 있도록 표시

1. 필요 최소한의 개인정보 수집 기준(정보통신망법 제23조제2항 관련)

◇ 개인정보 수집 목적을 명확히 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 수집

- ① 서비스 제공을 위해 반드시 필요한 “필수동의 항목”의 범위를 최소화하고, 그 외 선택동의 항목의 경우에는 별도로 개별적인 동의를 받아야 함
- ② 사전적·일괄적 수집을 제한하고 필요한 시점에 동의를 받아 수집

1. 기본 방향

□ [필수·선택동의 항목을 엄격하게 구분] 수집하는 개인정보의 항목을 필수동의 항목과 선택동의 항목으로 구분하여 최소한의 개인정보만을 수집·보관해야 함

○ (필수동의 항목은 최소한으로 설정) 서비스 제공에 필요한 최소한의 개인정보는 ‘해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보’로 엄격히 제한(개정 정보통신망법 제23조제3항, '14.11.29 시행)

※ 필수동의 항목 : 사업자가 이용자에게 서비스 제공을 위해 필수적으로 동의할 것을 요구할 수 있는 개인정보 항목으로, 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보에 한정

- ‘해당 서비스’는 사업자가 이용자에게 정보통신망을 통해 이용약관 등에 따라 제공하는 개별 서비스를 의미

※ 사업자와 이용자가 서비스 제공·이용 과정에서 합리적으로 예상 가능한 개별 서비스’를 의미

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

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

※ 해당 서비스의 본질적 기능과 필수항목(예시) : 참고①

o (선택동의 항목은 목적별로 개별 동의) 해당 개인정보 없이도 해당 서비스의 본질적 기능을 수행할 수 있는 경우에는 선택동의 항목으로 구분

- 선택동의 항목은 서비스 목적별로 나누어 “개별적으로 동의” 받도록 구성하여 이용자가 개인정보 제공여부를 선별적으로 결정

※ 서비스 목적을 지나치게 포괄적으로 기재하여 동의받지 않아야 함

- 특히, 마케팅 활용 목적을 위한 선택동의 항목(연락처 등)은 이용자가 명확히 알 수 있도록 별도로 분리하여 개별 동의

- 이용자가 동의를 거부하더라도 서비스 이용은 가능하다는 사실을 “굵은 글씨, 빨간색 등”으로 명확하게 표시하여 알 수 있도록 고지

※ (예시 ①) 맞춤형 광고 발송을 위한 연락처(이메일, 주소 등)는 필수동의 항목은 아니나, 선택동의 항목으로 분류하여 개별 동의를 받는 것은 가능

※ (예시 ②) 온라인 쇼핑물의 경우 결제·배송정보는 인터넷 회원가입 단계에서는 필수동의 항목으로 볼 수 없으나, 선택동의 항목으로 분류하여 이용자의 동의를 받은 경우에는 인터넷 회원가입 단계에서 수집·이용 가능

<필수동의 항목과 선택동의 항목의 구분(예시)>

구 분	필수동의 항목	선택동의 항목
개 념	· 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보 · 이용자에게 필수적 동의 요구 기능	· 사업자의 필요에 의해 수집하는 정보 · 이용자가 동의 여부를 선택 가능
예 시	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) 멤버십 할인 · (예시) 멤버십 정보(타사 이용정보)

※ 필수동의 항목은 해당서비스의 특성에 따라 다양하게 나타나므로, 예시의 해당 서비스를 제공한다고 하여 반드시 예시된 항목을 수집할 필요는 없음

☞ ‘본인확인 기능’이 해당 서비스의 본질적 기능인지 여부

- ▶ 해당 서비스 제공 과정에서 명의도용·개인정보 누출 등 방지를 위한 ‘본인확인’ 기능은 서비스의 특성에 따라 본질적 기능으로 분류할 수 있음
 - 다만, 본인확인 과정에서 수집한 개인정보는 본인확인 목적으로만 수집·이용 가능하고, 분쟁 발생시 증빙자료 등 필요 최소한의 개인정보만을 보관해야 함
- ▶ 회원가입 단계에서 불필요하게 본인확인을 강제하는 것은 바람직하지 않으며, 법령 상 의무이행(연령·본인확인 등)·명의도용 방지 등을 위해 필요한 경우라도 최소한의 개인정보만을 수집·보관해야 함
 - 수집한 개인정보를 다른 목적으로 이용하기 위해서는 반드시 별도로 이용자의 명시적 동의를 받아야 함

☞ 해당 서비스 제공에 필요한 필수동의 항목 설정 시 유의할 점

- ① 필수동의 항목은 해당 서비스의 특성에 따라 다르므로 예시된 필수항목(참고②)을 반드시 수집해야 하는 것은 아니며 해당 서비스의 특성에 맞게 결정해야 함
 - ※ (예시) 온라인 쇼핑몰에서 비회원 구매의 경우에는 ‘인터넷 회원가입’이 필요 없으므로 결제·배송 정보만을 수집
- ② 법령에 따라 동의없이 수집한 개인정보의 경우 법령이 정한 목적의 범위 안에서만 이용할 수 있으므로 별도 DB 또는 테이블에 분리하여 저장해야 하고 마케팅 등 다른 목적으로 이용할 수 없음
 - ※ 법정 수집 의무항목 및 보유기간(예시) : 참고②
- ③ 이용자의 개인정보를 다른 사업자로부터 적법하게(*) 제공받은 경우에는 이용자로부터 직접 수집하는 정보가 아니므로 정보통신망법 제22조에 따른 동의를 받을 필요는 없으나, 개인정보취급방침에 관련 내용을 기재하여 이용자가 언제든지 확인할 수 있도록 운영하는 것이 바람직
 - 다른 사업자로부터 이용자의 개인정보를 제공받는 경우에도 정보주체가 동의한 제휴 서비스의 종류와 범위 등에 대한 검토를 거쳐 반드시 필요한 최소한의 개인정보만을 제공받는 것이 바람직함
 - (*) 정보통신망법 제24조의2에 따라 개인정보를 제3자에게 제공하려는 자는 이용자의 동의를 받아야 함
- ④ 해당 서비스를 제공하기 위해 반드시 필요한 정보(필수동의 항목)의 경우에만 필수적으로 동의를 요구할 수 있도록 한 취지이므로, 사업자가 선택동의 항목에 대한 동의를 요청하고 이용자가 이에 선택적으로 동의한 경우에는 개인정보 수집·이용이 가능함

□ **[필요한 시점에 수집]** 이용자가 서비스를 실제 이용하는 시점에 수집·이용 동의를 받도록 하여 “미리” 동의를 받는 관행을 개선

- 서비스 개시를 위해 필요한 개인정보에 한정하여 수집·이용 동의를 받아야 하고, 이후에 제공되는 서비스의 경우 서비스 제공 시점에 동의를 받아야 함

※ (예시) 온라인 회원제 서비스의 경우 가입 시점에는 아이디, 비밀번호 등 최소한의 정보에 대한 동의를 요구하고, 이후 상품 구매 등 서비스 이용 단계에서 필요한 정보는 해당 시점에 동의를 요구할 수 있음

- 다만, 반복적인 서비스의 경우로서 최초 서비스 이용 시점에 선택 동의 항목으로 분류하여 동의를 받은 경우에는 수집·이용 가능

※ (예시) 온라인 쇼핑의 경우, 배송정보와 결제정보를 선택동의 항목으로 분류하여 향후 배송 및 결제서비스에 이용할 것을 동의받으면 수집·이용 가능

2. 해당 서비스의 단계별 수집 기준

□ 서비스 가입 단계

- **(온라인 회원가입)** 홈페이지를 회원제로 운영하는 경우, 회원 계정 생성을 위한 최소한의 개인정보(아이디, 비밀번호, 이름 등)만을 수집

- 이용자에게 제공하는 서비스와 무관하게 홈페이지를 회원제로 운영하고 그 과정에서 불필요한 개인정보를 수집하는 행위는 최소수집 원칙에 반함

※ (예시) 홈페이지를 이용하는 회원(준회원 포함)과 비회원의 서비스 이용 범위에 차이가 없는 경우 회원제 운영을 통한 불필요한 개인정보 수집에 해당

- 불필요하게 “이용자 본인확인”(휴대전화, 아이핀, 공인인증서, 기타)을 강제하면서 개인정보를 요구하는 것은 최소수집 원칙에 반함

※ (이용자 본인확인이 필요한 경우) ① 법률 상 의무이행(나이, 본인, 실명 확인 등), ② 서비스 특성 상 명의도용 등 이용자 피해 예방 등

☞ 정보통신망법 제31조의 “만14세 미만 아동 여부 확인”

- 인터넷 회원가입 단계에서 만14세 미만 아동 여부를 확인하기 위해 필요한 경우에는 이용자가 “법정 생년월일”을 직접 입력하도록 하고, 사업자는 이를 토대로 만14세 미만인지 여부를 확인하는 것이 바람직함
- 인터넷 회원가입 단계에서 만14세 미만 아동 여부의 확인만을 위해 본인확인(아이핀, 휴대전화, 공인인증서 등)을 강제하면서 불필요한 개인정보를 과다하게 수집하는 것은 최소수집 원칙에 반함
- 다만, 만14세 미만 아동을 직접 대상으로 하여 서비스를 제공하는 사업자의 경우에는 신뢰할 수 있는 방법으로 본인여부를 확인한 후 반드시 법정 대리인의 동의를 받아야 함

- “이용자 본인확인”이 필요한 경우에도 회원가입 단계에서 일률적으로 강제하는 것은 바람직하지 않으며, 필요한 시점에 본인확인을 요구하고 최소한의 개인정보를 수집하는 것이 바람직

※ 청소년보호법 등 법령에서 본인 또는 나이 확인을 요구하고 있는 경우에는 해당 서비스 이용 단계(성인용품 구매 등의 단계)에서 본인확인

○ (오프라인 회원가입) “해당 서비스”의 본질적 기능 수행에 필요한 개인정보를 필수동의 항목으로 명시하고 동의를 받아야 함

- 선택동의 항목은 이용자가 동의여부를 선택할 수 있도록 설정하여야 하며, 해당 서비스의 특성에 따라 사업자가 자율적 운영 가능
- 사업자가 서비스 신청자 본인 또는 정당한 대리인 인지 여부를 확인하기 위해 증빙서류를 수집하는 경우에도 확인만으로 가능한 경우에는 수집·저장하지 않아야 하고, 수집·저장이 필요한 경우에도 불필요한 정보는 마스킹 처리하여야 함

※ (예시①) 본인 여부 확인과 증빙을 위해 신분증(주민등록증 등)을 요구하는 경우, 단순 확인만으로 목적달성이 가능한 경우 별도의 사본을 저장해서는 안되며, 확인 증빙이 필요한 경우에도 불필요한 정보인 신분증 뒷면(지문, 주소), 주민등록번호 등은 마스킹 처리한 후 수집·저장하여야 함

※ (예시②) 요금감면 대상자인지 여부 확인을 위해 장애인등록증, 국가유공자 증빙서류 등을 수집하는 경우 확인 목적과 무관한 정보(민감정보 등)는 마스킹 처리한 후 보관

※ (예시③) 이용약관 상의 위약금 면제사유(이사 등) 확인을 위해 사업자가 요구하는 인사명령서, 주민등록등본 등의 서류는 담당자 확인 등으로 갈음하는 방안 등을 강구하는 것이 바람직

☞ 서비스 가입신청 시 주민등록번호의 수집 방법

- ① 법령 상 근거가 있는 경우, ② 본인확인기관으로 지정된 경우, ③ 방송통신위원회 고시에 의해 인정된 경우에는 주민등록번호를 수집할 수 있음
- 다만, 이 경우에도 가입신청서 상에는 주민등록번호 기재란을 삭제하고, 이용자에게 주민등록번호를 수집하는 근거와 목적을 명확하게 알리고 별도로 수집하는 것이 바람직함

○ (이 법 또는 다른 법률에 특별한 규정이 있는 경우) 이 법 또는 다른 법률 상 특별한 규정이 있으나, 수집항목이 포괄적으로 규정된 경우(*)에도 법이 규정한 목적 범위 안에서 최소한의 개인정보만을 수집·보관하기 위한 노력을 하여야 함

(*) 전자상거래등에서의 소비자보호에 관한 법률 제6조의 “거래기록” 등

<정보통신망법 제22조제2항에 따라 동의없이 수집하는 개인정보(예시)>

관련 법률	목적	수집항목(예시)	보유기간
통신비밀보호법 제15조의2 (통신사실확인자료)	법원의 영장을 받아 수사기관이 요청시 제공	로그기록, IP 등	3개월
		전기통신일시, 발신기지국의 위치추적자료 등	12개월
전자상거래등에서의 소비자보호에 관한 법률 제6조 (거래기록)	소비자의 불만 또는 분쟁처리	소비자 식별정보 분쟁처리 기록	3년
	계약 또는 청약철회 등에 관한 기록 등	소비자 식별정보 계약/청약철회 기록	5년

□ 서비스 이용 단계

- **(자동수집장치에 의해 수집하는 개인정보)** 서비스 계약 이행을 위해 필요하여 사업자가 서비스 제공 과정에서 자동수집장치에 의해 수집하는 개인정보(*)의 경우에도 최소수집 원칙이 적용

(*) 이용자 계정정보(개인 식별정보)와 결합된 인터넷 접속파일정보(쿠키정보, IP주소 등) 등

- 다만, 서비스 제공 과정에서 지속적으로 수집되는 특성으로 인해 매 시점마다 동의를 받는 것이 곤란한 경우에는 동의없이 수집 가능(*)하나, 이 경우에도 수집하는 개인정보의 항목·목적·보유기간을 특정하여 개인정보 취급방침에 명시해야 함

(*) 정보통신망법 제22조제2항제1호

☞ 해당 서비스 제공 계약 이행과는 무관한 목적으로 이용하기 위해 수집하는 경우, 선택동의 항목으로 분류하여 별도의 사전동의를 받아야 함

※ (예시) 쿠키를 통해 수집하는 행태정보를 분석하여 개인별 맞춤형 광고에 활용

- **(이용과정에서 수집·생성되는 개인정보)** 서비스 계약 이행을 위해 필요한 경우로서, 사업자가 서비스 제공 과정에서 수집·생성하는 이용내역정보의 경우에도 최소수집 원칙이 적용

- **(다른 법률에 따라 수집·보관하여야 하는 개인정보)** 이용자의 동의없이 수집 가능(*)하나, 법률이 정한 목적에 따라 최소한으로 수집하여야 함(전자상거래법 상의 '거래기록'등)

(*) 정보통신망법 제22조제2항제3호

- **(요금정산을 위해 필요한 개인정보)** 이용자의 동의없이도 수집 가능(*)하나, 요금정산을 위해 필요한 최소한의 정보만을 수집해야 함

※ 서비스 이용에 따른 요금액, 납부 또는 미납 사실 등이 이에 해당하며, 채권추심 등의 목적으로 요금정산과 무관한 정보를 수집할 수 없음

(*) 정보통신망법 제22조제2항제2호

2. 단계별 개인정보 파기 기준(정보통신망법 제29조 관련)

◇ 최소한의 개인정보만을 보관하도록, 수집·보관·제공·파기 단계별 개인정보 관리(파기) 기준을 제시함

- ① 수집·이용·제공 등의 목적과 보유기간을 특정하고 불필요한 개인정보는 **지체없이 파기**
- ② 법률에 의하여 수집이 허용된 개인정보 등은 **별도 분리 저장**한 후 파기사유 발생시 지체없이 파기
- ③ 이용자 편익·서비스 제공과 직접 관련이 없는 경우에는 **제3자 제공을 제한**하고, 파기 등 관리의무를 계약서에 반영

1. 개인정보 수집 단계

□ 목적 및 보유기간을 구체적으로 명시

- 목적과 보유기간을 구체적으로 명시하고, 파기 사유(목적 달성·보유기간 종료, 이용자 파기 요청) 발생 시에는 “지체없이” 파기
 - 목적을 ‘더 나은 서비스 제공을 위하여’, ‘서비스 개선을 위하여’와 같이 포괄적으로 제시하지 않아야 하고, 보유기간은 특정해야 함
 - 이용자가 명시적으로 자신의 개인정보 파기를 요청하거나, 수집·이용 동의를 철회한 경우 파기 처리절차를 명확히 해야 함

※ 개인정보취급방침에 파기 처리절차·방법을 명시(정보통신망법 제27조의2제2항제3호)

- 확인만으로 목적을 달성할 수 있는 경우에는 저장할 수 없음

☞ 본인여부 확인 정보

- ① 사업자가 본인확인이 필요하여 이용자에게 신분증(주민등록증, 운전면허증 등) 제시를 요구한 경우에는 확인만하고 저장하지 않도록 함

- 본인확인 사실에 대한 증빙이 필요한 경우라도 최소한의 확인 정보만 남기고 마스킹 처리하여 보관
 - 주민등록증 사본의 경우, 주민번호·발급일자·지문·주소 등 수집 동의를 받지 않은 개인정보는 보이지 않게 처리 후 저장
- ② 전화 고객센터 시 본인확인을 위해 수집한 개인정보는 본인확인이 끝나면 지체없이 파기

☞ 일회성 연락처 정보

- ① 일회성 서비스 제공을 위해 수집한 연락처 등의 정보는 수집 목적 달성시 지체없이 파기
- ② 케이블TV·초고속인터넷 방문설치, 배송을 위한 방문 등 일회성 목적으로 수집한 개인정보는 목적이 달성되면 지체없이 파기

□ 영업점의 개인정보 수집·보관 최소화

- o 통신사, 유료방송사 등 영업점을 운영하는 사업자(본사)는 영업점에서 보관하는 개인정보를 최소화하도록 개인정보 관리체계를 개편하고, 영업점에 대한 관리·감독을 주기적으로 실시해야 함

※ ‘영업점의 개인정보 보관 최소화 방안’을 마련하여 ‘개인정보를 안전하게 취급하기 위한 내부관리계획’에 반영

☞ 예시

- ① 영업점에서 이용자가 개인정보를 전자기기에 입력하면, 본사에 직접 전송되고 영업점에는 저장되지 않도록 하는 방안
- ② 영업점에 대한 주기적 개인정보 관리 실태점검 실시 방안
- ③ 본사가 텔레마케팅에 대한 이용자의 동의를 받은 경우라도, 본사가 지정한 영업점(텔레마케팅 업체 등)에 한하여 텔레마케팅을 할 수 있도록 엄격히 제한하여 영업점의 개인정보 이용 범위를 제한하는 방안 등

2. 서비스 이용·보관 단계

□ 서비스 이용 단계

- **(이용과정에서 수집·생성하는 정보)** 정보통신망법 제22조제2항 제1호에 따라 이용자의 동의없이 이용과정에서 수집·생성하는 정보의 경우에도 수집·이용 목적과 보유·이용 기간을 정하여 개인 정보취급방침에 공개해야 함
 - 개인정보취급방침에 공개한 수집·이용 목적과 보유·이용 기간이 종료된 경우에는 “지체없이” 파기
- **(동의 철회 정보)** 이용자가 개인정보 수집·이용 동의를 철회하는 경우, 법정 의무 이행을 위해 수집된 정보가 아닌 한 “지체없이” 파기해야 함

☞ 개정 정보통신망법 제30조 제3항('14.11.29.시행)

- 정보통신서비스 제공자등은 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 하여야 한다.

- **(접속기록, IP 등)** 통신비밀보호법에 따라 최소 3개월은 보유해야 함
 - 「유효기간제」(정보통신망법 제29조 제2항)에 따라 이용자가 정보통신 서비스를 이용하지 않은 기간을 확인하기 위해 필요한 ‘최종 접속 기록’은 ‘법령에서 정한 기간 동안’ 보관 가능함
 - 명의도용 피해자가 명의도용 사실 입증을 위해 접속기록, IP 등의 정보를 요청하는 경우와 같이 이용자 피해 구제를 위해 필요한 경우에는 이용자의 사전동의를 받은 후 동의받은 기간 동안 보관 가능
- **(민원상담 녹취록 등)** 이용자 민원 상담을 위해 저장한 녹취파일 등의 정보는 “보유기간 종료·목적 달성, 이용자 동의 철회 시” 파기
 - ※ 다만, 전자상거래등에서의 소비자보호에 관한 법률 상의 거래기록은 분쟁처리 기록(3년), 계약 또는 청약철회 기록(5년) 종료 후 파기

□ 개인정보 보관 단계

- **(별도 분리 보관)** 파기해야 할 개인정보는 서비스에 이용 중인 개인정보와 별도 분리하여 보관
 - 법률상 의무이행을 위해 보관이 필요한 경우 외부와 차단된 별도 DB 또는 테이블에 분리 보관하고 법률이 정한 목적 달성 또는 보유기간이 종료되면 재생할 수 없는 방법으로 파기
 - 이용자가 일정기간 서비스를 이용하지 않은 경우에는 재생할 수 없는 방법으로 파기하거나 별도 DB에 보관
- **(접근통제 강화)** 분리 보관된 개인정보는 관련 업무 담당자만 열람할 수 있도록 하고, 영업부서의 접근을 제한하여 외부 영업목적(텔레마케팅 등)으로 이용할 수 없도록 함

3. 제공 단계

- **(제3자 제공 제한 및 파기 확인)** 사업자가 무분별하게 개인정보를 제3자에게 제공하는 것을 제한하고, 제휴 서비스 관련으로 제공할 때에는 계약서에 파기 및 확인 사항을 명시하는 것이 바람직
- **(1단계)** 사업자가 무분별하게 개인정보를 제3자에게 제공하는 것을 원칙적으로 제한하고 예외적으로 허용
 - ※ (예외) 서비스 계약 이행과 관련이 있거나, 이용자 혜택과 관련이 있는 경우
- **(2단계)** 사업자가 제3자에게 개인정보를 제공한 경우, 이용자가 '해당 기업'과 '제3자'에게 선택적으로 파기 요청할 수 있어야 함
 - ※ '해당 사업자'에게 파기 요청하면 '제공받은 제3자'에게 파기 요청을 전달하고, 제3자는 파기하도록 함
- **(3단계)** 개인정보를 제3자에게 제공하고자 하는 기업은 계약서에 제공된 개인정보의 안전한 관리와 파기 및 확인 사항을 명시
 - ※ (계약서 반영내용) 개인정보에 대한 파기 의무, 기술적·관리적 보호조치 의무(고객 정보에 대한 접근 범위 설정, 암호화 보관 등) 등

- **(취급위탁 시 위탁자의 수탁자에 대한 파기 확인)** 사업자가 개인정보 취급을 수탁자에게 위탁한 경우, 수탁자가 실제 개인정보를 파기했는지 여부를 확인하여야 함
- **(1단계)** 사업자가 개인정보 취급을 위탁하고자 할 때에는 수탁자의 개인정보 보호조치 능력 등을 고려하여야 하고, 계약서에 개인정보 위탁 관련 사항을 포함하여 작성하여야 함
- **(2단계)** 사업자가 개인정보의 취급을 위탁한 경우, 이용자는 '해당 기업'과 '수탁자'에게 선택적으로 파기를 요청할 수 있고 해당 기업과 수탁자는 내부 업무연락을 통해 파기하여야 함
 - ※ 정보통신망법 제30조('14.11.29.시행)와 제67조 제2항에 따라 해당 사업자와 수탁자는 이용자의 파기 요청 시 파기의무 있음
- **(3단계)** 위탁 계약서에 위탁된 개인정보의 안전한 관리와 파기 및 확인 사항을 명시한 후 이행 여부를 **주기적으로 확인**해야 함
 - ※ (계약서 반영내용) 개인정보 파기·보호조치 관련 사항 외에 '주기적 확인'과 관련한 사항 포함 필요

4. 파기 단계

- **(파기시기)** 해당 목적을 달성한 경우, 보유·이용기간이 끝난 경우, 사업을 폐업하는 경우, 이용자가 동의를 철회한 경우에는 '지체 없이'(*) 개인정보를 파기하여야 함
 - (*) 안전행정부 「표준 개인정보보호 지침」 제11조제1항의 내용을 참고하여 정당한 사유(**)가 없는 한 5일 이내에 개인정보를 파기
 - (**) 후불제 서비스에서의 요금정산, 이용자의 요금 이의신청기간 운영, 법령에서 일정기간 보유하도록 규정한 경우 등
- **(파기방법)** 파기사유가 발생한 경우에는 '복구·재생할 수 없는 방법'으로 파기하여야 함

☞ 복구·재생할 수 없는 방법의 의미

- 사회 통념상 현재의 기술수준에서 적절한 비용이 소요되는 방법을 의미
- ※ 안전행정부 표준 개인정보보호 지침 제11조 제2항 참조

- (종이에 출력된 개인정보나 가입신청서 등) 인쇄물 등 파쇄가 가능한 형태인 경우에는 분쇄기 등을 이용하여 재조합이 불가능하도록 물리적으로 파쇄하거나 소각하여야 함
- (전자적 파일 형태인 경우) 하드디스크, CD/DVD, USB메모리 등의 매체에 전자기적으로 기록된 개인정보는 다시 재생시킬 수 없는 기술적 방법으로 삭제하거나 물리적인 방법으로 매체를 파괴하여 복구할 수 없도록 하여야 함
 - 파기할 때에는 원본 데이터 외에 백업 데이터가 존재하는지 여부를 확인하여 백업 데이터를 누락하는 사례가 없도록 주의해야 함

☞ 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 ‘로우레벨포맷(Low level format)’ 방법으로 파기
 - ※ 로우레벨포맷 : 하드디스크를 공장에서 나온 초기상태로 만들어주는 포맷
- ② 0, 1 혹은 랜덤한 값으로 기존 데이터를 여러 번 덮어쓰우는 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

3. 이해하기 쉬운 동의서 작성 기준(정보통신망법 제26조의2 관련)

◇ 일반인이면 누구나 특별한 주의를 기울이지 않아도 자연스레 이해가 가능하도록 표현

1. 동의를 받는 방법

□ (읽기 쉽게 동의서 개선) “법정 고지사항”만을 간결하게 고지하고, “쉬운 용어”, “중요내용은 부호, 색채, 굵고 큰 문자 등”을 활용하여 명확하게 표시

※ 불가피하게 전문용어를 사용하는 경우에는 별도의 용어 설명을 제공

○ (인터넷(PC기반) 동의) 인터넷을 통한 동의내용 고지는 비대면 동의의 특성을 고려하여 이용자가 최대한 이해하기 쉬운 방법을 마련

- 글자체와 글자크기는 이용 환경을 고려하여 선택하되, 이용자가 쉽게 읽을 수 있도록 조합

※ (예시) PC의 운영체제(OS)에서 기본적으로 지원되는 글자체를 사용하고, 글자크기는 웹사이트 구현시 기본크기 이상으로 설정

- 필수동의를 요구하는 사항(필수동의 항목, 약관 등)과 선택동의를 요구하는 사항(선택동의 항목, 취급위탁, 제3자 제공 등)을 순차적으로 구성하여 이용자가 이해하기 쉽도록 구성

- 화면 배경과 글자색 등은 이용자가 읽기 쉽도록 조합하여 사용하도록 권장

※ (예시) 흰색 배경에 글자색은 검은색 또는 진한 회색

○ (모바일 기기 등을 이용한 동의) 모바일 기기의 경우 PC 환경과는 달리 동의 화면이 작아 이용자에게 명확하게 고지하는 것이 어려움

- 모바일 기기에 보여줄 수 있는 최소한의 법정고지사항을 알리고 동의를 받되, 별도의 웹사이트를 운영하고 있는 경우에는 확인할 수 있는 방법을 안내하는 것이 바람직

○ (서면 동의) 글자크기, 줄간격 등을 확대하여 읽기 쉽게 개선

※ (예시) 항목구분 글자는 최소 12p, 본문글자 최소 10p, 줄간격 130% 이상

○ (전화 동의) 전화를 통해 개인정보를 수집하는 경우에는 ‘법정 고지 사항’을 ‘일상 대화 속도’로 설명하고 이해했는지 여부를 확인

□ (동의내용 고지 및 동의방법 개선) 이용자가 동의여부를 결정하고 자발적 의사에 따라 선택할 수 있는 방법을 마련해야 함

○ (필수동의 항목에 선택동의 항목 포함 금지) 필수동의 항목에는 해당 서비스의 본질적 기능 수행을 위한 개인정보 항목만을 포함

※ 그 외 사업자의 필요에 의해 수집하는 개인정보 항목은 선택동의 항목으로 분류하여 이용자가 동의 여부를 결정할 수 있도록 구성

○ (동의가 선택인 사항은 명확히 표시) 이용자가 동의 여부를 선택할 수 있다는 사실을 쉽게 확인할 수 있도록 ‘붉은색, 굵은 글씨 등’으로 표시

- 동의가 필수적인 사항과 선택적인 사항을 구분하여 순차적으로 동의를 요구하는 것이 바람직함

※ (예시) ① [필수] 필수동의 항목에 대한 수집·이용 동의→② [선택] 선택동의 항목에 대한 수집·이용 동의→③ [선택] 취급위탁 동의→④ [선택] 제3자 제공 동의

- 동의가 선택인 사항 중 “선택동의 항목”은 목적별로 이용자가 개별 동의 가능하도록 구성

※ 마케팅 목적으로 개인정보를 수집하는 경우 개별 동의 가능하도록 구성

<참고> 정보통신망법 상 개인정보 동의 요구 유형(예시)

유형	동의 요구 사례	관련 규정
동의를 필수인 사항	① 필수항목에 대한 개인정보 수집·이용 동의	제22조
	② 선택항목에 대한 개인정보 수집·이용 동의	제22조
동의를 선택인 사항	③ 개인정보 제3자 제공 동의	제24조의2
	④ 개인정보 취급위탁 동의(고지로 갈음하는 경우제외)	제25조

○ **(이용자가 직접 동의여부 선택)** 동의를 받을 때에는 “동의함”에 미리 표시할 수 없도록 함

※ 이용자가 동의여부를 능동적으로 결정할 수 있도록 하기 위하여, 선택 결과를 주어지게 구성(default 설정)하지 않아야 함

☞ **여러 동의사항에 대한 ‘일괄동의 기능’ 운영 가능**

- 이용자의 선택권이 보장된 경우에는 이용자 편의 제공을 위해 여러 동의사항에 대하여 일괄동의 기능을 도입하여 운영할 수 있음
- 다만, 일괄동의를 도입하더라도 이용자가 ‘동의내용을 확인한 후 개별동의가 가능하고, 일괄동의 여부는 강제가 아닌 선택사항이라는 점’을 명시적으로 알려야 함
- 일괄동의 기능은 선택동의 사항이 포함되어 있는 경우 선택동의 사항이 포함되어 있음을 알린 후 동의를 받아야 함

☞ **제휴서비스 제공을 위해 ‘제3자 제공’이 필수적인 경우 동의방법**

- 제휴서비스 중 이용자 포인트 적립과 같이 이용자 식별정보(예: 휴대전화번호)의 공유가 필수적인 경우에는 해당 사업자가 제3자인 제휴사업자에게 해당 식별정보를 제공하여야 제휴서비스를 이용자가 이용할 수 있음
- 이 경우, “개인정보 수집·이용 동의”를 받으면서 이용자가 동의 여부를 직접 표시하면 “제3자 제공 동의”에도 함께 표시되도록 구성하는 것은 가능(참고③ 참조)

※ 개인정보 수집·이용에 동의하였으나 제3자 제공에 동의하지 않은 경우에는 별도의 알림창을 통해 “동의하지 않으면 포인트 적립 등이 될 수 없음”을 알리고 재차 동의 요청 가능

○ **(동의하는 내용을 이해하기 쉽게 표시)** 개인정보 수집주체와 이용목적·항목·보유·이용기간을 연결하여 어떤 목적으로 수집·이용하고 언제까지 보관하는지 명확히 고지

- 일반인이 이해할 수 있을 정도의 “쉬운 용어”를 사용하도록 하고, 전문용어를 사용하는 경우에는 별도의 설명 제공
- 법정 고지사항을 간결하게 표시하여 동의 받도록 함
- 이용약관 동의, 개인정보 수집·이용 동의 등을 포괄적으로 받지 않도록 함

2. 동의를 받는 내용

□ **(동의 내용)** “법정고지사항”을 간결하게 표시하여 동의 받아야 하며, 그 외의 사항을 장황하게 포함하지 않도록 함

※ (잘못된 사례) ① 개인정보취급방침의 내용 전체를 고지하고 동의받는 방법,
② 이용자가 반드시 알아야 할 법정 고지사항 외의 내용을 서술하는 방법

< 법정 고지사항 >

구분	법정 고지사항 내용
수집·이용 동의	1. 개인정보의 수집·이용 목적 2. 수집하는 개인정보의 항목 3. 개인정보의 보유·이용 기간
제3자 제공 동의	1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간
취급위탁 동의	1. 개인정보 취급위탁을 받는자(수탁자) 2. 개인정보 취급위탁을 하는 업무의 내용

□ **(중요한 내용)** ‘굵은 글씨, 빨간색 등’으로 알아보기 쉽도록 표시

※ [중요한 내용] 사회적 통념에 비추어 고객이 계약체결의 여부나 대가를 결정 하는데 직접적인 영향을 미칠 수 있는 사항(대법원, 2008.12.16. 결정 2007마1328)

- **(수집·이용 동의)** 수집하는 항목 중 민감정보, 보유기간, 마케팅 목적 등은 이용자가 동의여부를 결정하는데 직접적인 영향을 미칠 수 있는 사항임
- **(제3자 제공 동의)** 제공되는 제3자, 마케팅 목적, 통상의 경우보다 장기의 보유기간 등을 포함하는 경우는 중요한 내용으로 볼 수 있음
 - “선택항목에 동의하지 않아도 서비스 이용이 가능하다는 사실”도 중요한 내용에 해당

◆ [명시적·실질적 동의의 조건]

- ① 형식적으로 “법정 고지사항”을 알리고 동의를 받았다고 하여 동의 획득 의무를 준수한 것으로 보기는 어려움
- ② 이용자에게 개인정보 수집·이용, 제3자 제공에 관한 동의를 구하고 있다는 사실 및 법정 고지사항을 명확히 알린 상태에서 이용자의 자발적 의사에 따라 동의 여부를 결정한 것으로 볼 수 있어야 함

참고①

해당 서비스의 본질적 기능과 필수동의 항목(예시)

해당 서비스	본질적 기능	필수동의 항목
인터넷 회원제 서비스	· 회원에 대한 요금조회, 상담(전화, 인터넷 등), 서비스 신청, 포인트 적립 등 · 명의도용·부정이용 방지 등 회원관리	아이디, 비밀번호(성명, 법정 생년월일, 연락처 등)
유료 서비스	· 구매한 서비스 및 상품 결제	결제수단 별 필요한 개인정보(계좌번호, 카드번호 등)
결제 및 배송 서비스	· 구매한 서비스 및 상품 결제, 배송	결제정보(계좌번호, 카드번호 등), 배송정보(배송 주소지, 수령인 연락처 등)
이동통신 서비스	· 휴대전화 개통-서비스 제공-이용 요금 정산-고객민원 상담 등 · 가입의사 확인·명의도용 방지 등 고객관리	이름, 법정 생년월일, 휴대전화번호, 단말기 정보, 요금결제정보(계좌번호, 카드번호 등), 요금 청구지 주소 등
SNS서비스	· 통신 및 정보전달 · 친구추천 등	이름, 휴대전화번호, 주소록(지인) 등
서비스 제공 과정에서의 법령 상 의무이행	· 정당한 이용자인지 여부 확인 · 연령에 따른 제한이 있는 경우 연령 확인	① 정보통신망법 제31조 - 만4세 미만 여부 확인을 위한 법정 생년월일 - 법정대리인 정보
		② 전기통신사업법 제29조 - 요금감면 대상자 확인을 위한 증명서류
		③ 청소년보호법 제23조의3 - 청소년(16세 미만) 여부 확인을 위한 법정 생년월일
		④ 청소년보호법 제16조 - 유해매체로부터 청소년 보호를 위한 법정 생년월일 및 본인 여부 확인 정보
		⑤ 게임산업진흥에 관한 법률 제12조의3 - 게임 중독 예방조치 의무 이행을 위한 법정 생년월일 및 본인 여부 확인정보 - 법정대리인 정보

※ 이해를 돕기위한 예시이므로 필수동의 항목(예시)이더라도 사업자의 해당 서비스 성격에 따라 판단해야 하며, 반드시 수집해야 하는 것은 아님

참고②
법정 수집 의무항목 및 보유기간 (예시)

관련 법률	목적	수집 항목(예시)	보유기간
통신비밀보호법 (통신사실확인자료)	법원의 영장을 받아 수사기관이 요청시 제공	로그기록, IP 등	3개월
		전기통신일시, 발신기지국의 위치추적자료 등	12개월
전자상거래등에서의 소비자보호에 관한 법률 (거래기록)	소비자의 불만 또는 분쟁처리	소비자 식별정보 분쟁처리 기록	3년
	계약 또는 청약철회 등에 관한 기록 등	소비자 식별정보 계약/청약철회 기록	5년
국세기본법	국세 부과 제척기간 계산	국세 증빙자료	10년
	국세징수권 등 소멸시효 계산	과세표준과 세액의 신고자료	5억이상 국세(10년) 그 외(5년)
전자금융거래법 (전자금융거래기록)	전자금융거래기록 확인	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

참고③

동의 사례 (예시)

■ [필수] 개인정보 수집·이용 동의

목적	항목	보유기간	동의여부
이용자 식별 및 본인여부 확인	성명, 아이디, 비밀번호, 비밀번호 힌트	회원탈퇴 후 5일까지	☐ 동의함 ☐ 동의안함
계약 이행을 위한 연락 민원 등 고객 고충 처리	연락처(이메일, 휴대전화번호)	회원탈퇴 후 5일까지	
만14세 미만 아동인지 확인	법정 생년월일	회원탈퇴 후 5일까지	

※ 000서비스 제공을 위해서 필요한 최소한의 개인정보이므로 동의를 해 주셔야 서비스를 이용하실 수 있습니다.

■ [선택] 개인정보 수집·이용 동의

목적	항목	보유기간	동의여부
새로운 상품 안내 마케팅(전화, 이메일)	휴대전화번호, 이메일	서비스 탈퇴 후 5일까지	☐ 동의함 ☐ 동의안함
맞춤형 광고	쿠키정보, 쿠키를 통해 수집되는 행태정보	서비스 탈퇴 후 5일까지	☐ 동의함 ☐ 동의안함
제휴서비스 이용시 포인트 적립 연계	휴대전화번호	제휴서비스 종료 후 5일까지	☐ 동의함 ☐ 동의안함
※ 아래 제3자 동의 항목의 (주)000에 대한 제3자 제공에도 동의해 주셔야 포인트 적립이 가능합니다.			

※ 동의를 거부하시는 경우에도 000서비스는 이용하실 수 있습니다.

■ [선택] 개인정보의 취급위탁에 대한 동의

수탁자	목적	동의여부
(주)000	위탁자((주)000)의 부가서비스 유치를 위한 마케팅 대행	☐ 동의 ☐ 동의안함

※ 동의를 거부하시는 경우에도 000서비스는 이용하실 수 있습니다.

■ [선택] 개인정보 제3자 제공에 대한 동의

제공 받는자	목적	항목	보유기간	동의여부
(주)000	제휴서비스 이용시 포인트 적립 연계	휴대전화번호	제휴서비스 종료 후 5일까지	☐ 동의함 ☐ 동의안함
(주)000 (판매자)	온라인 쇼핑 구매자에게 상품 배송	·구매자정보 : 아이디,이름, 주소,휴대전화번호 ·수령인 정보 : 이름, 휴대전화번호주소	배송 완료 후 5일까지	☐ 동의함 ☐ 동의안함

※ 동의를 거부하시는 경우에도 000서비스는 이용하실 수 있습니다.