개인정보 처리 위·수탁 안내서

2020.12.

개인정보보호위원회
KISA 한국인터넷진흥원

< 목 차 >

Ⅰ 안내서 개요

1. 발간 배경

o 개인정보 처리 위·수탁 이슈 증가

- IT업무의 아웃소싱 확대로 개인정보 처리 위·수탁 관련 이슈와 이에 대한 사회적 관심의 지속적 증가가 예상됨

o 개인정보 최소 수집 및 안전한 처리 요구 증가

- 매년 개인정보 유출사고가 발생하여 개인정보의 안전한 활용 및 최소 수집·처리에 대한 국민의 요구가 증가함

o 복잡한 개인정보 처리 위·수탁 관계에 따른 법·제도 안내 필요

- 「개인정보 보호법」 제26조의 의무를 보다 쉽게 이해할 수 있도록 위탁자 및 수탁자의 조치사항을 구체적으로 안내할 필요성 대두

2. 발간 목적

o 본 안내서는 개인정보 처리를 위·수탁할 때 위탁자와 수탁자가 알아야 할 조치사항을 위·수탁 단계별로 제시함

3. 안내서의 구성

o 개인정보 처리 위·수탁 시 개인정보 보호를 위해 이 안내서에서 소개하는 주요 내용은 다음과 같음

- 개인정보 처리 위·수탁 개념 및 판단기준
  1. 개인정보 처리 위·수탁의 개념
  2. 개인정보 처리 위·수탁의 판단 기준
- 위·수탁 단계별 조치사항
  1. 개인정보 처리 위·수탁 전
  2. 개인정보 처리 위·수탁 업무 수행 중
  3. 개인정보 처리 위·수탁 업무 종료 후
- 자주 묻는 질문(FAQ)

5. 안내서의 활용 및 저작권 표시

o 본 안내서의 저작권은 개인정보 보호위원회에 있음

o 본 안내서는 개인정보 처리 위·수탁 관련 위탁자와 수탁자가 취해야할 조치의 최소한의 기준을 제시함

o 누구나 개인정보보호 교육 및 안내 등의 목적으로 본 안내서를 활용(인용·편집 포함) 할 수 있으며

- 이러한 경우 아래와 같이 출처 및 저작권 표시

> * 출처 : 개인정보 보호위원회, 개인정보 처리 위·수탁 안내서(2020.12)

Ⅱ 개인정보 처리 위·수탁 개념 및 판단기준

1. 개인정보 처리 위·수탁의 개념

o 개인정보 처리 위·수탁이란 개인정보처리자(위탁자)가 개인정보 수집·이용 등의 처리 자체를 제3자(수탁자)에게 위·수탁하거나, 개인정보의 이용·제공 등 처리가 수반되는 업무를 수탁자에게 위·수탁하는 것을 의미

> 개인정보의 '처리위탁'은 본래의 개인정보 수집, 이용 목적과 관련된 위탁자 본인의 업무처리와 이익을 위하여 개인정보가 이전되는 경우를 의미(대법원 2017. 4. 7. 선고 2016도13263)

- '개인정보처리자'는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말함(「개인정보 보호법」 제2조 제5호)
- '업무'란 직업상 또는 사회생활상 지위에 기하여 계속적으로 종사하는 사무나 사업의 일체를 의미하는 것으로 단 1회의 행위라도 계속·반복의 의사가 있다면 업무로 볼 수 있음

※ 순수한 개인적인 활동이나 가사활동을 위해서 개인정보를 처리하는 자는 포함되지 않음

구분	업무위탁	제3자 제공
관련조항	「개인정보 보호법」 제26조	「개인정보 보호법」 제17조
예시	배송업무 위탁, TM 위탁 등	사업제휴, 개인정보 판매 등
이전목적	위탁자의 이익을 위해 처리	제3자의 이익을 위해 처리
예측 가능성	정보주체가 사전 예측 가능 (정보주체의 신뢰 범위 내)	정보주체가 사전 예측 곤란 (정보주체의 신뢰 범위 밖)
이전 방법	원칙 : 위탁사실 공개 예외 : 위탁사실 고지(마케팅 위탁)	원칙: 제공목적 등 고지 후 정보주체의 동의 획득
관리·감독 의무	위탁자	제공받는 자
손해배상책임	위탁자 및 수탁자 부담	제공받는 자 부담

2. 개인정보 처리 위·수탁의 판단 기준

o 개인정보 처리 위·수탁인지 여부의 판단 기준은 다음과 같음(대법원 2017.4.7. 선고 2016도13263판결 참고)

- 개인정보의 처리 위·수탁은 본래의 개인정보 수집·이용 목적과 관련된 위탁자 본인의 업무 처리와 이익을 위한 경우를 의미함

> (비교) 개인정보의 제3자 제공은 본래의 개인정보 수집, 이용 목적의 범위를 넘어 그 정보를 제공받는 자(제3자)의 업무 처리와 이익을 위하여 개인정보가 이전되는 경우를 의미하므로, 위탁자의 업무 처리 및 이익을 위한 개인정보 처리 위·수탁과 구분

- 어떠한 행위가 개인정보의 제공인지 아니면 처리위탁인지는 개인정보의 취득 목적과 방법, 대가 수수 여부, 수탁자에 대한 실질적인 관리감독 여부, 정보주체 또는 이용자의 개인정보 보호 필요성에 미치는 영향, 이러한 개인정보를 이용할 필요가 있는 자가 실질적으로 누구인지 등을 종합하여 판단

> 개인정보 처리위탁에 있어 수탁자는 위탁자로부터 위탁사무 처리에 따른 대가를 지급받는 것 외에는 **개인정보 처리에 관하여 독자적인 이익을 가지지 않고, 정보제공자의 관리·감독 아래 위탁받은 범위 내에서만 개인정보를 처리**하게 되므로, 개인정보 보호법 제17조와 정보통신망법 제24조의2에 정한 '제3자'에 해당하지 않음(판례 발췌)

Tip **위탁과 제3자 제공의 구분**

위탁과 제3자 제공을 구분하기 위해서는 대법원 판례와 같이 개인정보의 취득 목적과 방법, 대가 수수여부 등을 종합적으로 고려하여야 합니다. 위탁과 제3자 제공을 구분하는 중요한 기준은 개인정보 처리로 인한 업무수행 성과가 주로 누구에게 귀속되는지 입니다. 예를 들어 A기업(이하 '갑')과 B기업(이하 '을')이 개인정보 처리 업무를 포함하는 계약을 했으며 이를 토대로 '을'이 개인정보를 처리하더라도 해당 업무가 주로 '갑'의 업무 영역에 포함되어 있고 '을'이 처리하는 개인정보에 대한 지배·관리권이 여전히 '갑'에게 있다고 보이는 경우, 즉 '을'이 실제로 개인정보를 처리하더라도 '갑'의 이름으로 처리된다고 볼 수 있으면 개인정보 처리 위·수탁 관계에 해당합니다. 그러나 만약 해당 개인정보 처리가 '갑'보다는 '을'의 업무 영역으로 이해되고 그 업무 성과가 '을'에게 주로 귀속되는 경우에는 제3자 제공으로 보아야 할 것입니다.

<참고> 위·수탁 업무 사례

위탁자	수탁자
① 고객 대상 만족도 조사를 하려는 (가)기업	① (가)기업과 계약을 맺고 고객 리스트를 제공받은 A 컨설팅 회사
② 홈페이지를 운영하며 개인정보를 수집하는 (나)공공기관	② (나)공공기관의 사이트 관리를 수행하는 B업체
③ 인사 관련 문서를 파기하려는 (다)기업	③ (다)기업의 인사 문서를 파기하기 위해 고용된 C파쇄업체
④ 기업 공식 SNS의 활성화를 위해 D마케팅 업체와 계약한 (라)기업	④ (라)기업이 제공한 개인정보를 분석하여 고객의 성향을 고려한 친구 맺기 독려 캠페인을 진행하는 D마케팅 업체
⑤ 공공기관이 제공하는 자동 출금 서비스를 통해 기부금 관리를 하는 (마)대학	⑤ (마)대학으로부터 기부자의 정보를 받아 자동 출금 서비스를 제공하는 E공공기관
⑥ 등록금을 은행을 통해 대리 수납하는 (바)대학	⑥ (바)대학으로부터 재학생 정보를 받아 등록금 납부 서비스를 운영하는 F은행
⑦ 회사 내 직원 복지의 일환으로 리조트와 계약을 맺은 (사)기업	⑦ (사)기업으로부터 직원의 성명, 전화번호 등을 받아 객실 예약을 하는 G리조트
⑧ 전국에 약 천여개의 가맹점을 가지고 배달음식을 파는 (아)본사	⑧ (아)본사의 콜센터·홈페이지를 통해 접수된 배달주문을 처리하는 H가맹점
⑨ 도서 대출 반납 기기를 설치·운영하는 (자)시립도서관	⑨ 도서관 대출반납 처리기기를 유지보수하는 I업체
⑩ 파본도서를 교환해 주려는 (차)서점	⑩ (차)서점으로부터 고객 개인정보를 받아 도서를 새로 배송하는 J출판사
⑪ 역내 보안 CCTV 관제센터를 설립·운영중인 (카)구	⑪ (카)구의 보안 CCTV 관제센터를 24시간 모니터링하는 K보안업체
⑫ 채권추심업무를 외부로 위탁하려는 (타)기업	⑫ (타)기업으로부터 채무자 정보를 받아 추심업무를 하는 L채권회수전문기관
⑬ 회사에서 직원교육을 위해 교육 전문업체와 계약을 맺은 (파)기업	⑬ (파)기업으로부터 직원의 이름, 사번, 휴대폰 번호를 받아 교육을 수행하는 M교육업체
⑭ 공공기관 간 협약을 통해 업무 일부를 N공공기관에 위탁하는 (하)공공기관	⑭ 협약에 따라 (하)공공기관으로부터 개인정보를 전송받아 처리하는 N공공기관

Ⅱ 위·수탁 단계별 조치사항

본 안내서에서는 개인정보 처리 위·수탁을 **(1단계)개인정보 처리 위·수탁 전 (2단계)개인정보 처리 위·수탁 업무 수행 중 (3단계)개인정보 처리 위·수탁 업무 종료 후**의 3단계로 구분

- (1단계)는 위탁자가 수행하는 일련의 업무 중 위탁할 단위 업무를 구분하고 이를 수행할 수탁자를 선정하는 단계
- (2단계)는 수탁자에 의해서 개인정보가 처리되고 이를 위탁자가 감독하는 단계
- (3단계)는 개인정보 처리 업무가 종료되고 수탁자가 개인정보를 파기하거나 위탁자에게 반환하는 단계

<개인정보 처리 위·수탁 단계 요약>

단계	세부내용
개인정보 처리 위·수탁 전	개인정보 처리 위탁 업무 및 수탁자 선정
	개인정보 위·수탁 문서 작성
개인정보 처리 위·수탁 업무 수행 중	위탁자의 수탁자 관리·감독 및 수탁자의 개인정보 처리
개인정보 처리 위·수탁 업무 종료 후	수탁자의 개인정보의 파기·반환 및 위탁자의 파기 등 확인

1. 개인정보 처리 위·수탁 전 조치 사항

Step 1		Step 2		Step 3		최종
위탁할 업무 범위 구분	→	수탁자의 선정	→	처리 범위의 명확화	⇒	위·수탁 문서 작성
위탁 시 위험 고려 후 업무 위탁 여부 및 범위 결정		개인정보 보호 역량을 고려한 수탁자 선정		개인정보 수집 이용 최소화를 위한 위수탁자간 개인정보 처리 범위 명확화		위·수탁 문서를 통해 개인정보 보호 활동의 체계적·지속적 수행

o (위탁할 업무 범위 구분) 위탁자는 자신의 업무 중 위탁하여 수행할 업무를 선정하기 전, 개인정보 처리 위탁 시 발생할 수 있는 위험을 평가하여 업무 위탁 여부 및 범위를 결정해야 함

개인정보 처리 위탁 시 고려해야 할 개인정보 위험 요인(예시)

① 상세한 개인정보의 처리를 위·수탁하는 경우 개인정보 유출 및 오남용 시 피해가 큼
(예 : 주소 중 '도/시'보다 '도/시/도로명/상세주소'의 경우 피해가 큼)

② 민감정보의 처리를 위·수탁하는 경우 유출 및 오남용 시 피해가 큼
(민감정보 : 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력자료에 해당 하는 정보)

③ 대량의 개인정보를 처리하는 경우 개인정보 유출 및 오남용 시 피해가 큼

개인정보 처리 업무 위탁에 따른 위험성 평가 지표(예시)

위탁 시	평가 지표
위험성 증가	개인정보 유출 사고 발생 시 정보주체 프라이버시 침해 정도가 높은 경우(민감정보 처리 등)
	개인정보 유출 사고 발생 시 정보주체에게 경제적 손실을 야기할 수 있는 경우(금융정보 처리 등)
	개인정보 유출 사고 발생 시 다수의 정보주체가 피해를 입을 것으로 예상되는 경우(대량의 개인정보 처리 등)
안전성 증가	수탁자가 전문적인 보안관리 시설을 통해 개인정보 보호가 가능한 업무인 경우
	위탁자에 비하여 수탁자가 개인정보 보호 전문가를 많이 보유하고 위탁 업무에 투입할 수 있는 경우
	위탁자에 비하여 수탁자가 개인정보 관련 인증을 획득하는 등 공인된 개인정보 보호 활동을 잘 수행하는 경우
	수탁자가 가명조치 및 암호화 등 기술을 적용하여 개인정보를 잘 처리할 수 있는 업무인 경우

※ 해당 지표는 예시로, 사용 시 각 위탁자의 사정에 맞게 수정 활용 가능

- 개인정보 유출 시 위험성이 높다고 평가된 경우 위탁 범위에 대한 재검토, 위·수탁시 안전 조치 및 감독 강화, 위험요인 발생 시 책임 명확화 등 대책 강구가 필요함

- 또한 국외 위탁 시, 개인정보 위험 최소화를 위하여 수탁자가 속한 국가의 개인정보 보호 수준(감독기관의 존재, 개인정보 보호 관련 법률의 수립 및 시행 여부 등)을 함께 고려하는 것이 바람직함

o (수탁자의 선정) 위탁자는 수탁자의 개인정보 보호 역량을 종합적으로 검토하여 개인정보 위험을 최소화 할 수 있는 자를 선정하는 것이 바람직함

수탁자 개인정보 보호 역량 분석 평가 지표(예시)

평가 지표	
관리적 보호 수준	내부관리계획을 수립하고 정기적으로 현행화
	개인정보처리시스템에 대한 정기적인 위험평가 실시
	개인정보취급자에 대한 보안 각서 징구 및 개인정보보호 교육 실시
기술적 보호 수준	물리적·기술적 보호조치를 마련
	개인정보처리시스템에 침입차단 및 침입탐지 시스템 구축
	개인정보처리시스템에 대한 접근 권한 및 접근 이력 관리
물리적 보호 수준	주요 개인정보 처리 관련 설비에 대한 보호구역 지정 및 관리
	개인정보처리시스템에 대한 출입통제, 보안, 저장매체 등 관리
	개인정보취급자의 업무 환경에서 개인정보 보호를 위한 보안 관리 등 실시 여부 정기 점검
기타	PIMS 등 정보보호 및 개인정보보호 인증 획득 여부

※ 해당 지표는 예시로, 사용 시 각 위·수탁자의 사정에 맞게 수정 활용 가능

o (처리 범위 명확화) 위탁자는 수탁자가 위·수탁 업무 수행에 필요한 최소한의 개인정보를 처리하도록 해야 함

최소한의 개인정보를 위·수탁하지 않은 사례
① (의료 분야) 건강검진기관이 정보주체가 의뢰한 특정 검사를 외부 업체가 분석하도록 위탁할 때, 해당 분석과는 무관하거나 분석 목적에 과도한 정보인 정보주체의 생체정보, 문진표 등 검진기관이 보유한 거의 모든 검진 관련 정보를 수탁자에게 제공하는 경우
② (교육 분야) 아동을 대상으로 하는 학습지를 판매하는 회사가 이를 배송할 때, 학습지 수령에 필요한 배송정보(수령인인 부모 성명, 주소, 전화번호, 우편번호 등)뿐만 아니라 학습지를 공부할 아동의 이름, 나이, 학교 정보까지 택배회사에 제공하는 경우
③ (마케팅 분야) 마트 경품 이벤트 업무를 위탁하는 경우 이벤트 대행사가 고객으로부터 응모권을 통해 고객 이름, 연락처 뿐만 아니라 경품 배송 주소 및 제세공과금 처리를 위한 주민등록번호까지 미리 수집한 경우

o (위·수탁 문서 작성) 「개인정보 보호법」 제26조 제1항에 의하여 개인정보 처리 위·수탁은 반드시 문서에 의하여야 함(이하 위·수탁 문서)

- 위·수탁 문서에는 다음의 내용이 반드시 포함되어야 함

위·수탁 문서에 포함되어야 하는 내용	근거
① 위탁업무의 목적 및 범위	시행령 §28① 제1호
② 위탁업무 수행 목적 외 개인정보 처리 금지에 관한 사항	법 §26① 제1호
③ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항	시행령 §28① 제4호
④ 개인정보의 기술적·관리적 보호조치에 관한 사항 ※ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항	법 §26① 제2호 시행령 §28① 제3호
⑤ 재위탁 제한에 관한 사항	시행령 §28① 제2호
⑥ 수탁자가 준수하여야할 의무를 위반한 경우 손해배상 등 책임에 관한 사항	시행령 §28① 제5호

- 위·수탁 문서는 형식을 불문하므로 기업 간 협약서, 개인정보보호 약정서 등 다양한 문서 양식을 사용할 수 있음

- 위·수탁 문서는 반드시 별도로 작성하여야 하는 것은 아닌 바, 계약서 등에 위·수탁 시 포함되어야 하는 6가지 내용만 포함되어 있다면, 별도의 위·수탁 문서는 작성하지 않아도 됨

- 개인정보 보호위원회와 KISA는 사업자의 이해를 돕기 위하여 다음과 같이 표준 개인정보처리위탁 계약서를 위·수탁 문서의 예시로 제공 (별첨3)

- 업무 위·수탁 계약이 갱신되는 경우, 위·수탁 문서의 내용 재검토 및 수정 필요

Tip	업무 위탁 계약 절차 내 개인정보 처리 위 · 수탁 확인 절차 마련

업무 위탁 계약 시, 개인정보에 대한 인식이 부족한 현업 담당자들이 해당 업무에 개인정보 처리 위·수탁이 동반되는지 여부를 판단 하기는 쉽지 않습니다. 따라서 업무 위탁 계약 절차 내 개인정보 보호 담당 부서의 결재선을 추가 하는 등 개인정보 처리 위·수탁이 사전에 파악될 수 있는 절차를 마련하여 개인정보 처리 위·수탁에 따른 위험을 최소화해야 합니다.

<이것만은 꼭 기억하세요!>

1. 개인정보 처리를 위 · 수탁할 때는 반드시 문서에 의하여야 합니다. (법 제26조 제1항)

⇒ 이를 어길 시, 법 제75조 제4항에 의하여 1천만원 이하의 과태료 처분을 받을 수 있습니다.

현장점검 사례

① 위·수탁 문서에 법적 의무 사항 미포함한 경우>

현장사례	A병원은 연매출 100여 억원, 상시 종업원 160여 명 규모의 종합 병원으로, 수많은 환자들의 차질 없는 진료를 위하여 홈페이지와 EMR(Electronic Medical Record, 전자 의무 기록) 시스템을 운용하고 있다. 그리고 환자들의 개인정보가 포함된 전산 정보 처리 시스템의 유지 보수를 위하여 B업체와 개인정보처리 위·수탁 계약을 맺고 있다. 그러나 현장점검 결과, A병원과 B업체 간의 위·수탁 문서(이 사례에서는 위·수탁 계약서를 사용)상 법정 필수 기재 사항 중 일부 항목이 누락된 것을 확인할 수 있었다. 위·수탁 문서의 경우 필수 법적 의무 사항(목적 외 처리 금지, 기술적·관리적 보호 조치 및 접근 제한 등 안전 조치, 목적·범위, 재위탁 제한, 관리·감독 사항, 손해 배상 등 책임에 관한 사항)을 빠짐없이 모두 반영하여 작성하여야 하며, 이 중 한 항목이라도 누락될 경우 개인정보 보호법 위반에 해당한다.
위반사항	이 사례에서 A병원은 환자들의 개인정보가 포함된 전산 정보 처리 시스템 유지 보수를 위하여 B업체와 위·수탁 계약을 맺었는데, A병원과 B업체 간의 위·수탁 계약서에 기재하여야 할 법정 필수 기재 사항 중 개인정보의 처리 제한 항목을 누락한 상태로 위·수탁 계약서를 작성하였으므로 법 제26조 위반에 해당한다.
위반에 따른 벌칙	위반행위 : 업무 위탁시 법 제26조제1항 각호의 내용이 포함된 문서에 의하지 아니한 자 벌칙 : 1천만원 이하 과태료(법 제75조제4항제4호)
행정 처분	위·수탁 계약서 내 법적 의무 사항을 포함하도록 시정조치 및 1천만원 이하 과태료

2. 개인정보 처리 위·수탁 업무 수행 중 조치 사항

1) 위탁자

□ 위탁에 관한 사항을 정보주체에게 알릴 의무

「개인정보 보호법」 제26조 제2항 및 제3항

- ② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 '위탁자'라 한다)는 **위탁하는 업무의 내용**과 **개인정보 처리 업무를 위탁받아 처리하는 자**(이하 '수탁자'라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 **공개**하여야 한다.
- ③ 위탁자가 재화 또는 서비스를 **홍보하거나 판매를 권유하는 업무를 위탁하는 경우**에는 대통령령으로 정하는 방법에 따라 **위탁하는 업무의 내용**과 **수탁자**를 **정보주체에게 알려야** 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다

o 위탁자는 위탁하는 업무의 내용과 수탁자를 아래의 방법을 통해 공개해야 함

공개의 방법(개인정보보호법 시행령 제28조 제2항 내지 제3항)

(원칙) 위탁자의 인터넷 홈페이지를 통한 지속적 게재

(예외) 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 4가지 중 하나의 방법으로 공개

· 위탁자의 사업장 등의 보기 쉬운 장소에 게시

· 관보(위탁자가 공공기관인 경우에만 해당)나 위탁자의 사업장 등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷 신문에 싣는 방법

· 같은 제목으로 연2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법

· 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에 발급하는 방법

o 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 함

□ 수탁자에 대한 교육 및 감독 의무

「개인정보 보호법」 제26조 제4항

◆ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 **교육**하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 **감독**하여야 한다.

o 위탁자는 수탁자에 대하여 개인정보 보호 교육을 실시해야 함

- 교육의 방법 및 횟수 등은 수탁자의 개인정보보호 역량, 위·수탁 업무의 성격, 개인정보 위험, 위·수탁 기간 등을 고려하여 위탁자와 수탁자가 협의하여 결정하는 것이 바람직함

Tip	수탁자 개인정보 보호 교육의 시행

법 제26조 제4항에 의한 위탁자의 수탁자 교육은, 위탁자가 직접 실시하는 것이 원칙입니다. 다만 예외적으로 위탁자는 제3자인 개인정보 보호 교육 전문가, 전문 교육 기관 등을 통해 수탁자를 교육할 수 있습니다. 이러한 경우 위탁자는 교육의 내용, 시간 등을 고려하여 수탁자가 실질적으로 개인정보보호 역량을 높일 수 있도록 해야 합니다. 또한 수탁자 스스로 개인정보 보호 교육을 실시할 수 있습니다. 이 경우 수탁자는 교육을 수행하기 전 사전에 위탁자와 협의하고 위탁자가 요구하는 교육을 받았음을 증빙할 수 있어야 합니다.

o 위탁자는 수탁자가 법 제26조 제1항 각호의 사항 및 제29조의 안전조치의무를 준수하는지 여부 등 개인정보 처리 현황을 감독해 야 함

감독의 범위 및 방법
<감독의 범위> 「개인정보 보호법」 제26조 제4항 및 동법 시행령 제28조 제6항에 의해서 위탁자의 수탁자에 대한 감독의 범위는 법 제26조 제7항에 의한 수탁자의 의무와 법 제26조 제1항에 의해 위·수탁 문서에 명시된 내용의 이행 여부임. 즉 위탁업무 수행 목적 외 개인정보를 처리하는지 여부, 개인정보의 기술적·관리적 보호조치가 적절한지 여부 등 개인정보 위험 요인을 체계적·지속적으로 관리하여야 함
<감독의 방법> 위탁자가 수탁자를 감독하는 방법에 대하여 법률에 특별히 규정된 바는 없으므로 자료제출 요구, 현장 방문, 점검 도구 배포 등 합리적인 수단을 다양하게 활용할 수 있음.

- 위탁자는 수탁자의 개인정보 처리 현황에 대한 감독을 위하여 수탁자와 협의하여 정기적 보고를 요청할 수 있음

o 위탁자는 실질적인 감독을 위하여 감독 계획을 미리 수립하고 이를 수탁자와 협의하는 것이 바람직함

- 위탁자는 업무의 위탁 기간, 성격, 개인정보의 유형 등을 고려하여 정기적으로 수탁자의 개인정보 관리 실태를 점검하는 것이 바람직함

Tip	감독 및 교육 의무 이행의 방법

① 위탁자는 자체 감독 계획을 세워 수탁자를 관리하는 것이 좋습니다. 예를 들어 위-수탁자간 개인정보 전송량 및 수탁자의 개인정보 처리량 등을 기준으로 수탁자의 개인정보 위험성을 등급화 한 뒤 현장 점검, 원격 점검 등 다양한 수단을 합리적으로 사용하여 감독을 시행할 수 있습니다.

※ 감독 계획(예시) : 사전평가 → 수탁자 분류(등급화) → 체크리스트를 통한 수탁자 자체 점검 → 수탁자 이행계획서 제출 → 위탁자 현장점검 및 원격 점검 → 감독 결과 도출 및 사후 조치

② 택배, 결제대행 등의 특정 업종에서는 수탁업무를 주로 수행합니다. 따라서 이러한 업종의 사업자들은 다수 위탁자의 감독 및 교육에 대응해야 하는 부담을 지닙니다. 합리적인 감독의 수행을 위하여 수탁자는 사전에 위탁자들과 협의하여 전문 기관(관련 협회, 컨설팅 기관 등)의 점검을 통해 감독 및 교육을 대행할 수 있습니다.

Tip	감독 및 교육 의무 이행의 방법

③ 또한, 위탁자는 수탁자에 대한 개인정보 관리 지원을 통하여 감독을 수행할 수 있습니다. 특히 수탁자가 영세한 경우 이러한 감독의 방법이 유효합니다. 예를 들어 개인정보보호 솔루션 배포, DRM 기술 적용 등을 통해 수탁자의 개인정보 보호 역량을 강화하고 동시에 위탁자의 관리 감독을 쉽게 할 수 있습니다.

④ 해외에 있는 수탁자를 감독해야 하는 경우에는 위탁자가 직접 감독·교육을 하기 어려울 수 있습니다. 이 경우에는 대리인을 통해 할 수 있습니다. 다만 수탁자와 협의하여 계약서와 위·수탁 문서, 감독·교육 계획에도 대리인을 통한 감독·교육을 명시하는 것이 바람직합니다.

현장점검 사례

② 개인정보 처리 업무 수탁사 및 위탁 업무 공개 미흡

현장사례	국내 임대 및 건설 관련 업무를 하고 있는 B업체는 대표 홈페이지, 시설 관리 시스템, 분양 임대 관리 시스템의 유지 보수를 위하여 C, D, E 업체와 각각 개인정보처리 업무 위·수탁 계약을 맺고 있다. B업체는 이와 관련하여 대표 홈페이지에 '개인정보의 위탁 처리'라는 항목으로 고객의 개인정보를 외부에 위탁 처리하고 있음을 공개한 상태였다. 그러나 현장점검 결과, 위탁 처리와 관련하여 정작 중요한 위탁 업무 내용과 수탁자에 대해서는 어떠한 정보도 담고 있지 않다는 것을 알 수 있었다. 이 경우 구체적인 개인정보처리 업무의 위탁 내용과 함께 해당 업무의 수탁사인 C, D, E 업체에 대해서도 홈페이지에 분명하게 공개하여 고객, 즉 정보주체가 이를 언제든지 쉽게 확인할 수 있도록 하여야 한다.
위반사항	개인정보처리 업무위탁에 대하여 위탁하는 업무 내용과 업무를 위탁받아 처리하는 수탁자를 공개하지 않았고, 개인정보의 처리 업무를 위탁하는 내용만 공개하였으므로 법 제26조제2항 위반에 해당한다.
위반에 따른 벌칙	위반행위 : 업무위탁에 따른 개인정보처리 사실을 공개하지 아니한 자(법 제26조제2항) 벌칙 : 1천만원 이하 과태료(법 제75조제4항제5호)
행정 처분	위탁 업무 공개에 관한 시정조치 및 1천만원 이하 과태료

③ 개인정보처리 업무 위탁에 따른 법적 의무를 사항 이행하지 않은 경우

현장사례	C리조트는 휴가철과 같은 성수기에는 리조트 정회원들의 예약이 많고, 비수기에는 비회원들의 예약이 많은 편이어서 특별히 한쪽에 치우치기보다는 이들을 모두 아우를 수 있는 전략을 수립하고 있다. 그래서 리조트 회원들의 개인정보를 관리하는 통합 정보 관리 시스템과 함께 홈페이지를 통하여 비회원들도 회원 가입을 할 수 있는 홈페이지 시스템을 별도로 구축하여 운용하고 있다. 그러나 C리조트가 통합 정보 관리 시스템과 홈페이지 시스템을 제대로 운영할 수 있는 여력이 없어, 이 둘을 각각 D, E업체에 위탁하는 형태로 유지·보수 계약을 맺었다. 그러나 현장점검 결과, C리조트는 개인정보처리 업무의 위·수탁 계약 체결 이후, 수탁사인 D, E업체에 대하여 개인정보의 안전한 처리를 위한 교육을 정기적으로 실시하지 않았을 뿐 아니라, 개인정보처리 현황에 대한 점검 등의 관리·감독 의무도 소홀히 하고 있던 것으로 나타났다. 비록 수탁자에게 해당 업무를 일임한다고 하더라도 위탁자인 C리조트는 고객의 개인정보가 수탁자에 의해 안전하게 처리되는지에 대한 관리·감독 및 교육의 책임이 있다 .
위반사항	개인정보처리 업무를 위탁하는 개인정보처리자는 수탁자에 대한 관리·감독과 더불어 안전한 개인정보처리를 위하여 정기적으로 교육을 진행하지 않았으므로 법 제26조제4항 위반에 해당한다.
위반에 따른 벌칙	위반행위 : 수탁자가 개인정보를 안전하게 처리하는지 감독하지 아니한 자(제26조제4항) 준용규정 : 수탁자에 관해서는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.
행정 처분	개인정보처리 업무의 수탁자 관리 감독 관련 시정조치

□ 위탁자의 법적 책임(별첨1 참고)

① 행정 책임

o 위탁자는 수탁자가 법령을 위반한 경우에도 법 제61조, 제63조, 제64조에 의하여 개선권고 등 행정기관의 감독을 받으며, 법 제75조에 의하여 과태료 처분을 받을 수 있음

② 민사 책임

o 위탁자는 법 제26조 제6항에 의하여 수탁자의 위법한 행위로 인해 정보주체에게 손해가 발생할 경우 배상 책임을 짐

<이것만은 꼭 기억하세요!>

1. 개인정보 처리 위·수탁이 이루어지면 위탁자는 **업무의 내용**과 **수탁자를 홈페이지 등에 공개**하여야 합니다.(법 제26조 제2항)

⇒ 이를 어길 시, 법 제75조 제4항에 의하여 **1천만원 이하의 과태료** 처분을 받을 수 있습니다.

2. 재화 또는 서비스 **홍보나 판매 권유 업무**를 위탁하는 경우에는 **서면, 전자우편, 팩스, 전화, 문자전송 등의 방법**으로 **업무의 내용**과 **수탁자**를 **정보주체에게 알려야** 합니다.(법 제26조 제3항)

⇒ 이를 어길 시, 법 제75조 제2항에 의하여 **3천만원 이하의 과태료** 처분을 받을 수 있습니다.

3. 위탁자는 **수탁자를 교육하고 감독**해야 합니다.(법 제26조 제4항)

4. 수탁자가 **불법적으로 개인정보를 유출**하는 경우, 위탁자는 정보주체에 대해여 **손해배상 책임**을 집니다.(법 제26조 제6항)

2) 수탁자

□ 법 제26조 제7항의 의무 이행

o 수탁자는 개인정보 처리 시 법 제26조 제7항에 의하여, 개인정보 처리자에게 부여된 일반적인 의무를 이행해야 함

「개인정보 보호법」 제26조 제7항

◆ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

수탁자의 의무 주요 내용 요약	
개인정보 수집 및 제공 (법 제15조~제19조)	수탁자는 개인정보 수집·이용 시 위·수탁 문서 상 명시된 개인정보 처리 목적 범위 내에서 이용할 수 있으며, 위탁자 혹은 정보주체로부터 필요 최소한의 개인정보를 수집하여야 함. 또한 위·수탁 목적 범위를 초과하여 개인정보를 이용하거나 제3자에게 개인정보를 제공할 수 없음
정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지 (법 제20조)	수탁자는 정보주체의 요구가 있으면 개인정보의 수집 출처 및 처리 목적, 처리정지 요구권이 있다는 사실을 정보주체에게 알려야 함
개인정보의 파기 (법 제21조)	수탁자는 개인정보 보유기간이 경과되거나 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 된 때에는 지체 없이 개인정보를 파기해야 함
개인정보의 처리 제한 (법 제23조~제25조)	수탁자는 법령에 특별 규정이 없는 한 민감정보와 고유식별정보(특히 주민등록번호)는 처리할 수 없으며, 영상정보처리기기 역시 특별한 사유가 없는 한 설치·운영할 수 없음
정보주체의 권리 행사 보장 (법 제35조~제37조)	정보주체는 수탁자에게 개인정보의 열람, 정정·삭제, 처리정지를 요청할 수 있으며, 수탁자는 특별한 사정이 없는 한 이에 응해야 함

- 특히, 수탁자에게도 법 제29조의 안전조치 의무가 적용되므로 개인정보 보호를 위한 물리적/기술적 조치를 다 하지 않은 경우 처벌을 받을 수 있음(별첨2 참고)

개인정보의 안전성 확보조치

① 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
② 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
③ 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
④ 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
⑤ 개인정보에 대한 보안프로그램의 설치 및 갱신
⑥ 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

□ 수탁자의 법적 책임(별첨 2 참고)

o 수탁자는 법령 위반이 있는 경우에 개인정보 보호위원회 등의 자료 제출 요구 및 검사(제63조), 시정조치 등의 명령(제64조)에 응하여야 함

o 수탁자는 법령 위반이 있는 경우에 징역 또는 벌금(제70조부터 제73조까지), 몰수추징(제74조의2) 등의 형사책임을 부담할 수 있음

o 수탁자는 법 위반의 사유로 정보주체에게 손해를 입힌 경우에는 손해배상 책임을 질 수 있음(민법 제750조)

3) 개인정보 처리 재위탁시 준수할 사항

□ 원칙

o 개인정보 처리 업무의 재위탁은 개인정보 유출 등의 위험성을 높이므로 최소한의 범위로 한정하여야 함

- 특히 개인정보 위험을 증가시키는지, 정보주체의 권리에 불이익한 영향을 미치는지 등을 미리 검토하여 재위탁 하는 것이 바람직함

□ 위탁자 조치 사항

o 위탁자는 법 제26조 제4항에 의하여 재수탁자를 교육하고 개인정보 처리 현황을 감독할 의무가 있음

- 다만, 교육 및 감독의 방법에 있어 수탁자와의 사전 협의를 통해 합리적인 수준으로 다양한 방법을 활용할 수 있음

o 위탁자는 법 제26조 제2항에 의하여 재위탁하는 업무의 내용과 재수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개해야 함

- 다만, 홈페이지 내 링크(예 : 수탁사의 개인정보처리방침 링크 등)를 통한 공개 등 다양한 수단을 활용할 수 있음

□ 수탁자 조치 사항

o 개인정보 처리를 재위탁하려는 수탁자는 재위탁 사실을 위탁자에게 미리 알리고 동의를 받아야 함

o 수탁자는 재수탁자와의 관계에서는 민법 제756조의 사용자 책임을 부담하게 되므로 재수탁자에 대한 관리·감독 의무가 있음

□ 재수탁자 조치 사항

o 재수탁자는 수탁자와 동일하게 법 제26조에 의한 개인정보 보호를 위한 모든 조치를 수행해야 함

<이것만은 꼭 기억하세요!>

1. **수탁자는 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 됩니다. (법 제26조 제5항)**

=> **이를 어길시, 법 제71조에 의하여 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해질 수 있습니다.**

3. 개인정보 처리 위·수탁 업무 종료 후 조치 사항

1) 위탁자

o 위탁자는 수탁자가 개인정보를 파기하였는지를 확인하고 그에 대한 증빙자료를 가지고 있는 것이 바람직함

- 파기의 방법, 시기, 절차 등은 사전에 수탁자와 협의하여 위·수탁 문서 작성 시 이를 반영하는 것이 바람직함

2) 수탁자

o 위·수탁 문서에 명시된 개인정보 처리 기간이 종료되면 수탁자는 위탁자에게 개인정보를 반환하거나 지체 없이 파기하여야 함

- 계약 기간 내라도 위·수탁 문서에 명시한 개인정보 처리 목적이 사라지는 경우는 개인정보를 위탁자에게 반환하거나 지체 없이 파기하여야 함

파기의 방법
수탁자는 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 다음 중 어느 하나의 조치를 하여야 함 ① 완전파괴(소각·파쇄 등) ※ 예시 : 종이문서, 하드디스크나 자기테이프는 파쇄기로 파기하거나 용해, 또는 소각장, 소각로에서 태워서 파기 ② 전용 소자장비를 이용하여 삭제 ※ 예시 : 디가우저(Degausser)를 이용해 하드디스크나 자기테이프에 저장된 개인정보 삭제 ③ 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행 ※ 예시 : 개인정보가 저장된 하드디스크에 대해 완전포맷(3회 이상 권고), 데이터 영역에 무작위 값(0, 1 등)으로 덮어쓰기(3회이상 권고), 해당 드라이브를 안전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등

3) 위·수탁 업무 종료 후 개인정보의 추가 처리

o 위·수탁 업무 종료 후라도 법률상 의무 이행, 민원 등의 목적으로 개인정보의 보관 등 추가 처리가 필요한 경우, 위·수탁 문서에 해당 내용을 명시하는 것이 바람직함

Tip	위·수탁 업무 종료 후 개인정보 보관 등 추가 처리가 필요하다면?

① 법령상 개인정보의 보관 의무는 없으나 민원 등의 처리를 위하여 수탁자가 개인정보를 보관해야할 필요가 있는 경우

- 위·수탁 문서에 수탁자가 개인정보를 보관하는 기간과 목적 등을 사전에 명시하여야 합니다.

② 법령상 개인정보를 보관해야 하며 해당 의무가 위탁자에게 발생하는 경우

- 위탁자는 위·수탁 업무가 종료된 경우에 수탁자로부터 개인정보를 반환받아 보관하는 것이 원칙입니다. 다만 위·수탁 문서를 통해 수탁자가 보관하도록 미리 정할 수 있고, 이 경우에는 법률의 근거, 수탁자가 개인정보를 보관하는 기간과 목적 등을 위·수탁 문서에 명시하여야 합니다.

③ 법령상 개인정보를 보관해야 하며 이 의무가 수탁자에게 발생하는 경우

- 수탁자가 법령에 근거하여 개인정보를 보관하는 경우에는 위탁자에게 이러한 사실을 미리 알려야 합니다. 위·수탁 문서 내에 법률상 근거, 개인정보를 보관하는 기간과 목적 등을 사전에 명시하여야 합니다.

<이것만은 꼭 기억하세요!>

1. **수탁자는 「개인정보 보호법」 제26조 제7항 및 제21조에 의하여 개인정보 파기 의무를 집니다. 따라서 수탁자는 개인정보 처리 위·수탁 업무 종료 후에는 반드시 개인정보를 파기하거나 위탁자에게 반환하여야 합니다.**

<개인정보 처리 위·수탁 단계별 주요 조치사항>

<table>
<tr><th>단계</th><th>주요 내용</th></tr>
<tr><td>계약 전</td><td>
o 위험도 분석 등 예방조치를 통한 개인정보 유출 위험 최소화
- 위·수탁하는 개인정보의 가치, 유출 사고 시 정보주체가 입는 피해 정도 등 개인정보 위험 평가를 통한 위·수탁 대상 업무 구분
- 수탁자로 인한 개인정보 위험 최소화를 위하여 관리적, 기술적, 물리적 관점에서 수탁자 개인정보 보호 역량 종합 평가
- 위·수탁 업무 수행에 필요한 최소한의 개인정보 목록을 위탁자와 수탁자 간 사전 협의하여 개인정보 처리 범위 및 책임소재 명확화
- 개인정보 위험의 체계적·지속적 관리를 위한 위·수탁자 주요 협의 사항 문서 작성(「개인정보 보호법」 제26조 제1항)
</td></tr>
<tr><td>업무 수행 중</td><td>
o 개인정보 위·수탁에 따른 위탁자 및 수탁자의 주요 의무 사항 명확화
<table>
<tr><th>위탁자</th><th>수탁자</th></tr>
<tr><td>
- 수탁자의 개인정보 관리 체계, 기술적·물리적 보호 조치의 적절성 여부 감독
※ 자료 제출 요구, 현장 방문, 시스템을 통한 원격 점검 등 다양한 수단 활용 가능
- 수탁자 대상 개인정보 보호 교육
※ (원칙) 위탁자 직접 교육 (예외) 외부 전문가, 수탁자 자체 교육 후 증빙 확인
</td><td>
- 「개인정보 보호법」 제26조 제7항에 의한 의무 이행
※ 특히 법 제29조의 안전조치 의무 적용
- 수탁자 고의 또는 과실로 정보주체에 피해를 입힌 경우 손해 배상 책임
- 개인정보 처리 재위탁은 위·수탁 문서에 근거해야 함
</td></tr>
</table>
</td></tr>
<tr><td>업무 종료 후</td><td>
o 위·수탁 종료 시 지체 없는 개인정보 파기(반환)를 통한 개인정보 불법 처리·유통 방지
- 위·수탁 문서에 명시된 개인정보 처리 기간이 종료되거나, 사업 중이라도 개인정보 처리 목적이 달성된 경우 지체 없는 파기(5일)가 원칙
- 수탁자는 위탁자 요청 시 개인정보를 즉시 반환하며, 이 경우 개인정보의 무결성 및 완전성을 보장
- 위탁자는 수탁자의 개인정보 파기 여부 확인 후 증빙 자료를 남겨야 함
</td></tr>
</table>

Ⅳ 자주 묻는 질문(FAQ)

Q1 수탁업체의 개인정보 보유 기간도 공개해야 하나요?

「개인정보 보호법」 제26조 제2항에 의하면 개인정보 처리 위·수탁 시 위탁자는 위탁하는 업무의 내용과 수탁자를 홈페이지 공개 등 정보주체가 언제든지 쉽게 확인할 수 있도록 공개해야 합니다. 따라서 법률상 수탁자의 개인정보 보유 기간을 공개할 의무는 없습니다. 다만 이를 위·수탁 문서에 적절히 반영하는 것이 필요합니다. 또한 수탁자의 개인정보 처리기간은 위탁자가 정한 기간을 초과할 수 없습니다.

Q2 개인정보 처리 위·수탁 시 정보주체의 동의를 받아야 하나요?

「개인정보 보호법」 제26조 제2항은 개인정보 처리 위·수탁 시 위탁 업무의 내용과 수탁자를 공개하도록 되어있을 뿐 별도의 동의는 요구하지 않습니다. 또한 동조 제3항에 의하면 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법에 의하여 정보주체에게 위탁하는 업무의 내용과 수탁자를 알려야 합니다. 따라서 「개인정보 보호법」에 의하면 개인정보 처리 위·수탁 시 정보주체의 동의를 받을 필요는 없습니다.

Q3 법령에 근거가 있어 동의 없이 수집·이용한 개인정보의 처리를 위탁할 경우에도 위·수탁 문서에 의하여야 하나요?

「개인정보 보호법」 제15조 제1항은 개인정보 수집·이용의 근거로 정보주체의 동의, 법령에 수집 근거가 있는 경우 등을 규정하고 있습니다. 동법 제15조와 제26조는 별개의 조항이므로 제15조 제1항의 적용이 제26조의 적용을 배제하는 것은 아닙니다. 따라서 제15조에 의한 개인정보 수집·이용의 근거와 관계없이 개인정보의 처리를 위·수탁 한다면 위·수탁 문서를 반드시 작성해야 합니다.

Q4	수탁자가 다수 있는 경우 감독을 어떻게 하나요?

수탁자에 대한 감독이 반드시 수탁자의 개인정보 처리 현장에 대한 위탁자의 직접 방문을 뜻하는 것은 아닙니다. 감독의 방법 및 범위가 「개인정보 보호법」의 취지에 비추어 합리적이라면 현장 점검을 비롯하여 원격 점검 등 감독의 방법은 자율적으로 택할 수 있습니다. 또한 위탁자가 수탁자의 개인정보 보호 역량, 개인정보 위험 등을 고려하여 정할 수 있습니다.

Q5	수탁자에게 교육 비용을 부담시킬 수 있나요?

「개인정보 보호법」 제26조 제4항은 교육 비용에 대해서 특별히 규정하고 있지 않습니다. 따라서 교육 비용에 대해서는 위·수탁 문서에 이를 명시하고 위탁자와 수탁자간 사전 협의를 통해 결정하는 것이 바람직합니다.

Q6	「개인정보 보호법」 제26조 제7항에 의해서 동법 제20조가 수탁자에게 준용되는데, 위탁자로부터 개인정보를 제공받은 수탁자는 정보주체에게 수집 출처 등을 알려야 하나요?

「개인정보 보호법」 제20조 제1항의 입법 취지는 개인정보를 본인이 아닌 제3자로부터 수집하여 처리하는 경우 정보주체가 수집·이용 목적 등을 쉽게 알기 어려울 수 있으므로 정보주체의 요구가 있을 때 출처 등을 고지하도록 한 것입니다. 따라서 수탁자는 정보주체의 요구가 있을 시 수집출처, 개인정보의 처리 목적, 제37조에 의한 개인정보 처리 정지 요구권의 존재를 정보주체에게 알려야 합니다.

다만, 「개인정보 보호법」 제20조 제2항은 동법 제17조 제1항 제1호의 제3자 제공의 경우에만 적용이 되므로 제26조의 개인정보 업무 위탁에는 적용되지 않습니다.

Q7	기업의 규모와 개인정보 보유량에 따라서 개인정보의 안전성 확보조치가 달리 적용되는데, 수탁자도 마찬가지 인가요?

개인정보 보호위원회 고시인 「개인정보의 안전성 확보조치 기준」 제3조에 의하면 개인정보처리자의 유형 및 개인정보 보유량에 따라 안전조치의 적용을 완화하거나 강화하고 있습니다. 개인정보 보유량이 많을수록, 기업의 규모가 클수록 더 강화된 안전성 확보조치를 하여야 합니다. 수탁자는 위탁자를 기준으로 별표1의 유형을 적용하는 것이 원칙이지만, 수탁자 자신이 처리하는 개인정보 보유량 전체를 고려하여 안전조치를 하는 것이 바람직합니다.

Q8	‘지체 없이 파기’의 시간적 기준을 알고 싶어요.

표준 개인정보 보호지침 제10조 제1항에 의하면 개인정보처리자는 처리목적이 달성되거나 해당 서비스 및 사업이 종료된 경우 자연재해 등 정당한 사유가 없는 한 5일 이내에 개인정보를 파기하여야 합니다. 따라서 수탁자도 개인정보 처리 목적을 달성한 경우에는 5일 이내에 파기하여야 합니다. 또한 위·수탁 계약 종료하거나 해지된 경우에는 위탁자와의 합의에 따라 지체 없이 개인정보를 파기하거나 반환하여야 합니다.

Q9	시스템에 대한 단순 유지 보수를 위탁하는 경우에도 개인정보 처리 위·수탁인가요?

개인정보 처리 시스템의 유지 보수를 외부에 위탁한 경우 개인정보 처리 위·수탁으로 볼 수 있습니다. 「개인정보 보호법」 제2조 제2호에 의하면 ‘처리란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 유사한 행위’로 규정하고 있습니다. 유지 보수는 저장 또는 보유 업무의 일부를 구성하고, 또한 그와 유사한 행위에 해당하는 것으로 볼 수 있습니다. 다만, 시스템의 부품만 교체하는 등 개인정보에 접근하지 아니하는 경우라면 개인정보 처리 위·수탁이 아닙니다.

Q10	플랫폼을 이용하여 개인정보를 처리하는 경우 플랫폼 제공 사업자를 수탁자로 볼 수 있나요?

플랫폼 제공 사업자가 개인정보 처리에 관여하지 않고, 개인정보 보호 의무가 모두 플랫폼을 이용하는 자에게 있다면 플랫폼 제공 사업자를 수탁자로 보기 어렵습니다. (예 : 행사 안내를 위해서 포털사이트에서 제공하는 초대장 발송 서비스를 이용하는 경우 등) 다만, 위·수탁 여부를 판단할 때 개인정보의 처리 목적, 방법 등을 종합적으로 고려하여 만약 플랫폼 제공 사업자에 의해 개인정보 분석 등의 처리가 일어나며 이러한 처리가 플랫폼을 이용하는 자의 지시·감독에 의한 경우에는 개인정보 처리 위·수탁으로 볼 수 있습니다.

Q11	우편이나 택배를 이용하는 경우 개인정보 처리 위·수탁인가요?

우편배달사업자나 인터넷서비스제공자 등이 다른 사람의 개인정보를 단순히 전달 또는 전송하는 업무를 수행하게 되는 경우는 개인정보 처리가 일어난다고 볼 수 없어 개인정보 처리 위·수탁이 아닙니다. (예 : 주소와 받는 사람이 적힌 연하장의 발송을 우체국에 맡기는 경우 등) 그러나 우편배달사업자 등에게 개인정보의 처리가 수반되는 배달 업무를 위탁하는 경우 개인정보 처리 위·수탁으로 볼 수 있습니다. (예: 홈쇼핑과 계약을 통해 택배사가 정기적으로 배송 업무를 수행하며 고객 관리를 하는 경우 등)

[별첨1] 위탁자의 법적 책임 주요 내용 요약

행정 책임	
의견제시 및 개선 권고 (법 제61조)	개인정보 보호위원회는 개인정보 보호를 위하여 필요하다고 인정하면 위탁자에게 개인정보 처리 실태의 개선을 권고할 수 있음. 이 경우 권고를 받은 위탁자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 개인정보 보호위원회에 알려야 함
자료제출 요구 및 검사 (법 제63조)	개인정보 보호위원회는「개인정보 보호법」위반 사항을 발견하거나 혐의가 있음을 알게 된 경우, 이 법 위반에 대한 신고나 민원을 받은 경우 등에 해당되면 위탁자에게 관계 물품·서류 등 자료를 제출하게 할 수 있음 또한 위탁자가 제1항에 따른 자료를 제출하지 않거나 이 법을 위반한 사실이 있다고 인정되면 소속공무원을 통해 위탁자·수탁자 혹은 관련자의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있음
시정조치 (법 제64조)	개인정보 보호위원회는 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 위탁자에 대하여 개인정보 침해행위의 중지, 개인정보 처리의 일시적인 정지, 그 밖에 개인정보 보호 및 침해 방지를 위하여 필요한 조치를 명할 수 있음
과태료 (법 제75조)	위탁자는 업무 위탁 시 문서에 의하지 아니하거나 업무의 내용과 수탁자를 공개하지 아니한 경우 1천만원 이하의 과태료를 부과 받을 수 있음

민사 책임	
일반 불법행위 책임 (민법 제750조)	위탁자는 법 제26조 제4항에 의하여 수탁자의 개인정보 처리에 대한 감독 의무가 있음. 만약 수탁자의 불법행위로 정보주체에게 손해가 발생하였고, 위탁자가 감독 의무를 충실히 이행하는 등 자신의 고의 과실이 없음을 입증할 수 없다면 위탁자는 민법 제750조에 의한 불법행위 책임을 짐
사용자 책임 (민법 제756조)	수탁자가 개인정보 보호법을 위반하여 발생한 손해배상책임에 대하여, 법 제26조 제6항에 의하여 수탁자는 위탁자의 소속 직원으로 간주되므로 선임 및 관리감독의무를 하지 않은 이상 위탁자에게 민법 제756조의 사용자 책임이 인정됨. 그러나 위탁자가 수탁자의 선임 및 그 사무 감독에 상당한 주의를 하였음에도 손해가 있을 경우에는 손해배상책임이 면책됨 **「개인정보 보호법」 제26조 제6항** ◆ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

[별첨2] 수탁자의 법적 책임 주요 내용 요약

행정 책임	
자료제출 요구 및 검사 (법 제63조)	개인정보 보호위원회는 --(생략)-- 소속 공무원으로 하여금 개인정보처리자 및 해당 법 위반사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있음. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 함
시정조치 (법 제64조)	개인정보 보호위원회는 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 수탁자에 대하여 개인정보 침해행위의 중지, 개인정보 처리의 일시적인 정지, 그 밖에 개인정보 보호 및 침해 방지를 위하여 필요한 조치를 명할 수 있음

민사 책임	
불법행위 책임 (민법 제750조)	수탁자가 고의 또는 과실로 인한 위법행위로 정보주체에게 손해를 입혔을 경우 불법행위에 대한 손해배상 책임을 짐
수탁자의 손해배상 의무	「개인정보 보호법」 제26조 제6항에 의해 위탁자가 지니는 민법 제756조의 사용자 배상 책임은 수탁자의 불법행위 책임의 소멸이 아닌 정보주체의 효율적 구제를 위한 것이므로, 수탁자의 불법행위 인한 정보주체의 손해에 대하여 위탁자가 사용자 배상 책임을 지더라도 수탁자의 불법행위 책임이 소멸하는 것이 아님. 따라서 정보주체는 수탁자에게 직접 손해배상을 청구할 수 있으며 위탁자가 구상권을 행사하는 경우 수탁자는 이를 보상해야 함

형사 책임	
벌칙 (법 제70조) **10년 이하의 징역 또는 1억원 이하의 벌금**	1. 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자 2. 거짓이나 그 밖의 부정한 수단이나 방법으로 다른 사람이 처리하고 있는 개인정보를 취득한 후 이를 영리 또는 부정한 목적으로 제3자에게 제공한 자와 이를 교사·알선한 자
벌칙 (법 제71조) **5년 이하의 징역 또는 5천만원 이하의 벌금**	1. 제17조 제1항 제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자 2. 제18조 제1항·제2항, 제19조, 제26조 제5항 또는 제27조 제3항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 3. 제23조 제1항를 위반하여 민감정보를 처리한 자 4. 제24조 제1항을 위반하여 고유식별정보를 처리한 자 5. 제59조 제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 6. 제59조 제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자
벌칙 (법 제72조) **3년 이하의 징역 또는 3천만원 이하의 벌금**	1. 제25조 제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자 2. 제59조 제1호를 위반하여 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자
벌칙 (법 제73조) **2년 이하의 징역 또는 2천만원 이하의 벌금**	1. 제23조 제2항, 제24조 제3항, 제25조 제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자 2. 제36조 제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자 3. 제37조 제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자
몰수·추징 등 (법 제74조의2)	제70조부터 제73조까지의 어느 하나에 해당하는 죄를 지은 자가 해당 위반 행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 이를 몰수할 수 없을 때는 그 가액을 추징할 수 있음. 이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있음

[별첨3] 표준 개인정보처리위탁 계약서(안)

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보 처리 업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서(안)

OOO(이하 "갑"이라 한다)과 △△△(이하 "을"이라 한다)는 "갑"의 개인정보 처리업무를 "을"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "갑"이 개인정보처리업무를 "을"에게 위탁하고, "을"은 이를 승낙하여 "을"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」, 같은 법 시행령 및 시행규칙,「개인정보의 안전성 확보조치 기준」(개인정보 보호위원회 고시 제2020-2호) 및「표준 개인정보 보호지침」(개인정보 보호위원회 고시 제2020-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "을"은 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1.
2.

제4조 (위탁업무 기간) 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.

계약 기간 : 20oo년 o월 o일 ~ 20oo년 o월 o일

제5조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "을"이 다른 제3의 회사와 수탁계약을 할 경우에는 "을"은 해당 사실을 계약 체결 7일 이전에 "갑"에게 통보하고 협의하여야 한다.

제6조 (개인정보의 안전성 확보조치) "을"은「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보 보호위원회 고시 제2020-2호)에 따라 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

하고 있는 개인정보를 「개인정보 보호법 시행령」 제16조 및「개인정보의 안전성 확보조치 기준」(개인정보 보호위원회 고시 제2020-2호)에 따라 즉시 파기하거나 "갑"에게 반납하여야 한다.

③ 제2항에 따라 "을"이 개인정보를 파기한 경우 지체없이 "갑"에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① "갑"은 "을"에 대하여 다음 각 호의 사항을 감독할 수 있으며, "을"은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속기록
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② "갑"은 "을"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "을"은 특별한 사유가 없는 한 이행하여야 한다.

③ "갑"은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 (__)회 "을"을 교육할 수 있으며, "을"은 이에 응하여야 한다[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "갑"은 "을"과 협의하여 시행한다.

제9조 (정보주체 권리보장) ① "을"은 정보주체의 개인정보 열람, 정정·삭제, 처리 정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① "을"은 제4항의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 "갑"에게 확인받아야 한다.

제11조 (손해배상) ① "을" 또는 "을"의 임직원 기타 "을"의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 "을" 또는 "을"의 임직원 기타 "을"의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 "갑" 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 "을"은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 "갑"이 전부 또는 일부를 배상한 때에는 "갑"은 이를 "을"에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, "갑"과 "을"이 서명 또는 날인한 후 각 1부씩 보관한다.

20 . . .

갑	을
○○시 ○○구 ○○동 ○○번지	○○시 ○○구 ○○동 ○○번지
성 명 : (인)	성 명 : (인)

2) 「개인정보의 안전성 확보조치 기준」(개인정보 보호위원회 고시 제2020-2호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

[별첨4] 개인정보의 안전성 확보조치 기준

개인정보의 안전성 확보조치 기준

[시행 2020. 8. 11.] [개인정보보호위원회고시 제2020-2호, 2020. 8. 11., 제정]

개인정보보호위원회(신기술개인정보과), 02-2100-3063

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제23조제2항, 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "대기업"이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
5. "중견기업"이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.
6. "중소기업"이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
7. "소상공인"이란 「소상공인 보호 및 지원에 관한 법률」 제2조에 해당하는 자를 말한다.
8. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
9. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
12. "비밀번호"란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
13. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신

또는 수신하는 정보통신체계를 말한다.

14. "공개된 무선망"이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
15. "모바일 기기"란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
16. "바이오정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
17. "보조저장매체"란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
18. "내부망"이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
20. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(안전조치 기준 적용) 개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 [별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다.

제4조(내부 관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근 권한의 관리에 관한 사항
5. 접근 통제에 관한 사항
6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보 보호를 위하여 필요한 사항

② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니

할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.
③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.
④ 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리 하여야 한다.

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.
③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.
⑥개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.
⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.
③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.
④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.
⑤개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.
⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에

서 제공하는 접근 통제 기능을 이용할 수 있다.
⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.
⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과
⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.
⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.
⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.
② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.
③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제9조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.
1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트

웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제10조(관리용 단말기의 안전조치) 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.
1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

제11조(물리적 안전조치) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제12조(재해·재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.
② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.
③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.
1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

제14조(재검토 기한) 개인정보보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2020-2호, 2020. 8. 11.>

이 고시는 고시한 날부터 시행한다.

[별첨5] 위-수탁자 개인정보보호 체크리스트

단계	번호	점검 사항	대상
계약 전	1	위탁자는 위탁할 업무의 개인정보 위험성을 확인하였는가?	위탁자
	2	위탁자는 수탁자의 개인정보 보호 역량을 확인하였는가?	위탁자
	3	위탁자는 위탁하여 처리할 개인정보의 범위를 명확히 하고 수탁자와 사전 협의 하였는가?	위탁자
	4	위-수탁자는 다음 6가지 내용이 포함된 위·수탁 문서를 작성하였는가? ① 위탁업무의 목적 및 범위 ② 위탁업무 수행 목적 외 개인정보 처리 금지에 관한 사항 ③ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항 ④ 개인정보의 기술적·관리적 보호조치에 관한 사항 ※ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 ⑤ 재위탁 제한에 관한 사항 ⑥ 수탁자가 준수하여야할 의무를 위반한 경우 손해배상 등 책임에 관한 사항	위탁자 수탁자
	5	만약 위·수탁 업무 종료 후에도 수탁자가 개인정보를 보관하는 등 추가 처리를 해야 하는 사유가 있다면 미리 위·수탁 문서에 이를 포함 하였는가?	
	6	만약 법령상 수탁자에게 개인정보를 보관해야 하는 의무가 발생하는 경우 위탁자에게 이를 미리 알리고 위·수탁 문서 내에 법률상 근거와 개인정보 보관 기간·목적 등을 명시하였는가?	
업무 수행 중	7	위탁자는 위탁 업무 내용과 수탁자를 홈페이지 등에 공개하였는가?	위탁자
	8	위탁자는 수탁자의 개인정보 처리가 안전한지 여부를 감독하기 위한 계획을 수립하고 시행하였는가?	위탁자
	9	수탁자는 법 제29조의 안전조치 의무를 다하였는가? ① 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 ② 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치 ③ 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 ④ 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 ⑤ 개인정보에 대한 보안프로그램의 설치 및 갱신 ⑥ 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치	수탁자
	10	위탁자는 수탁자 대상 개인정보보호 교육을 위한 계획을 세우고 시행하였는가?	위탁자
	11	위탁자와 수탁자는 개인정보 열람·정정·파기 요청 등 정보주체의 권리 행사를 보장하기 위한 창구를 마련하였는가?	위탁자 수탁자
업무 종료 후	12	수탁자는 개인정보 파기 사유가 발생한 경우 지체 없이 이를 파기하였는가?	수탁자
	13	위탁자는 수탁자의 개인정보 파기를 확인하였는가?	위탁자

[별표] 개인정보처리자 유형별 안전조치 기준

개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

유형	적용 대상	안전조치 기준
유형1 (완화)	· 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제5조 : 제2항부터 제5항까지 · 제6조 : 제1항, 제3항, 제6항 및 제7항 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형2 (표준)	· 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 · 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제4조 : 제1항제1호부터 제11호까지 및 제 15호, 제3항부터 제4항까지 · 제5조 · 제6조 : 제1항부터 제7항까지 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형3 (강화)	· 10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체	· 제4조부터 제13조까지

개인정보 처리 위·수탁 안내서

발 행 일 2020. 12.

발 행 처 개인정보보호위원회 한국인터넷진흥원

디자인·인쇄 한결엠 02-6952-0551

중증장애인생산품생산시설

사회적협동조합

사회적기업