믿을 수 있는 개인정보 활용, 신뢰사회의 기본입니다.

Privacy by Trust, Trust by Privacy

개인정보 처리업무 위·수탁시 준수사항

Contents

Ⅰ 처리단계별 보호조치

Ⅱ 위탁자가 준수해야 할 사항

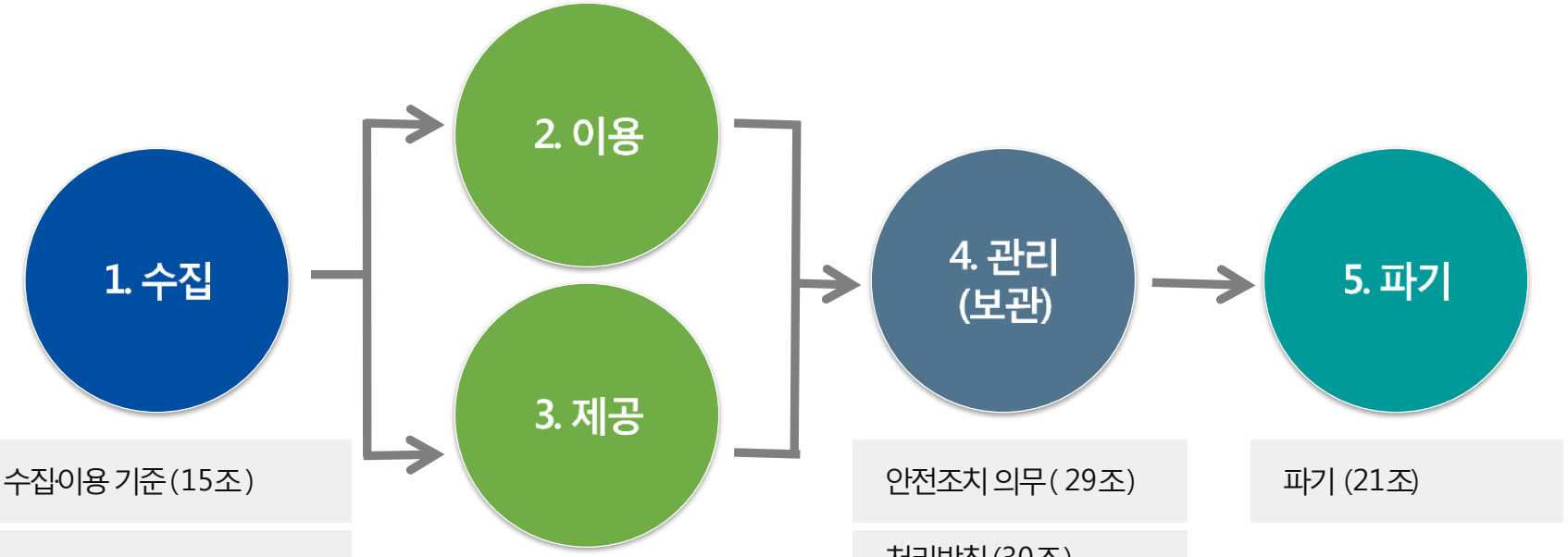
Ⅲ 수탁자가 준수해야 할 사항

I 처리단계별 보호조치

개인정보 보호 원칙 (법 제3조)

1. 처리 목적의 명확화, 목적 내에서 **적법하고 정당하게 최소 수집**
2. 처리 목적 내에서 처리, **목적 외 활용 금지**
3. 처리 목적 내에서 **정확성·완전성·최신성** 보장
4. 정보주체의 **권리침해 위험성 등을 고려**하여 안전하게 관리
5. 개인정보 처리사항 공개, **정보주체의 권리보장**
6. **사생활 침해 최소화** 방법으로 처리
7. 가능한 경우 **익명 처리**
8. 개인정보처리자의 책임 준수, 정보주체의 **신뢰성 확보**

개인정보 처리단계별 보호조치



- 수집·이용 기준 (15조)
- 최소 수집 (16조)
- 사전명시적 동의, 14세 미만 법정 대리인 동의 (22조)
- **- 처리제한 -** 민감정보 (23조), 고유식별정보 (24조) 주민번호 (24조의2)
- 영상정보처리기기(25조)

- 제3자 제공 (17조)
- 처리위탁 (26조)
- 영업양수도 (27조)
- 개인정보제공 (17조)
- 목적외 이용·제공 (18조)

- 안전조치 의무 (29조)
- 처리방침 (30조) 보호책임자 (31조)
- 개인정보 유출 시 통지·신고 (34조)
- 개인정보 파일 등록 (32조)
- 개인정보영향평가 (33조)

- 파기 (21조)

Ⅱ 위탁자가 준수해야 할 사항

문서(계약서)로 계약

개인정보 처리업무의 위탁은 문서(계약서)에 의해서 해야 함

(법 제26조 제1항, 시행령 제28조 제1항)

계약서에 포함되어야 할 내용

① 위탁업무 수행 목적 외 개인정보의 처리 금지

② 개인정보의 기술적·관리적 보호조치

③ 위탁업무의 목적 및 범위

④ 재위탁 제한

⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치

⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등의 감독

⑦ 수탁자가 준수해야 할 의무를 위반한 경우 손해배상 등의 책임

개인정보처리 위탁계약서(예시)

개인정보처리위탁 계약서(예시)

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 하는 데 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」(행정안전부 고시 제2017-1호) 및 「표준 개인정보 보호지침」(행정안전부 고시 제2017-1호)에서 정의된 바에 따른다.

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

1.

2.

제4조 (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.

제5조 (개인정보의 안전성 확보조치) "을"은「개인정보 보호법」제23조 제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조,「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2017-1호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (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 보유하고 있는 개인정보를「개인정보 보호법」시행령 제16조 및「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2017-1호)에 따라 즉시 파기하거나 "갑"에게 반납하여야 한다.

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

제7조 (수탁자에 대한 관리·감독 등) ① "갑"은 "을"에 대하여 다음 각 호의 사항을 감독 할 수 있으며, "을"은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
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

개인정보처리 위탁계약서(예시)

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·위조·변조 또는 훼손되지 아니하도록 1년에 (_)회 "을"을 교육할 수 있으며, "을"은 이에 응하여야 한다.

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

제8조 (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 ○○길 ○○		○○시 ○○로 ○○	
성 명 :	(인)	성 명 :	(인)

개인정보 처리방침에 공개

정보주체가 언제든지 쉽게 확인할 수 있도록 위탁 업무 내용과 수탁자를 공개해야 함
(법 제26조 제2항, 시행령 제28조 제2항 · 제3항)

※ 위탁사항이 있으면 **개인정보처리방침에 포함**시켜야 하므로(법 제30조 제1항), 이를 준수하면 이 조항은 준수하게 됨

인터넷 홈페이지가 있는 경우	위탁자의 인터넷 홈페이지(개인정보 처리방침)에 위탁 업무의 내용과 수탁자를 지속적으로 게재
인터넷 홈페이지가 없는 경우	① 위탁자의 사업장 등의 보기 쉬운 장소에 게시 ② 관보나 위탁자의 사업장 등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 일간신문, 주간신문 또는 인터넷신문 ③ 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적 게시 ④ 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급

[참고] 개인정보 처리방침에 기재할 사항

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부
4. 개인정보의 처리 및 보유 기간
5. 개인정보의 제3자 제공
6. 개인정보처리의 위탁
7. 개인정보의 파기에 관한 사항
8. 개인정보의 안전성 확보조치
9. 개인정보 처리방침의 변경
10. 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
11. 정보주체의 권익침해에 대한 구제방법

별도 통지해야 하는 경우

① **재화나 서비스를 홍보하거나 판매를 권유**하는 업무를 위탁하는 경우
② 위탁 **업무 내용이나 수탁자가 변경**된 경우

알리는 방법

① 개별통지: 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법
② 위탁자의 과실 없이 위의 방법으로 정보주체에게 알릴 수 없는 경우

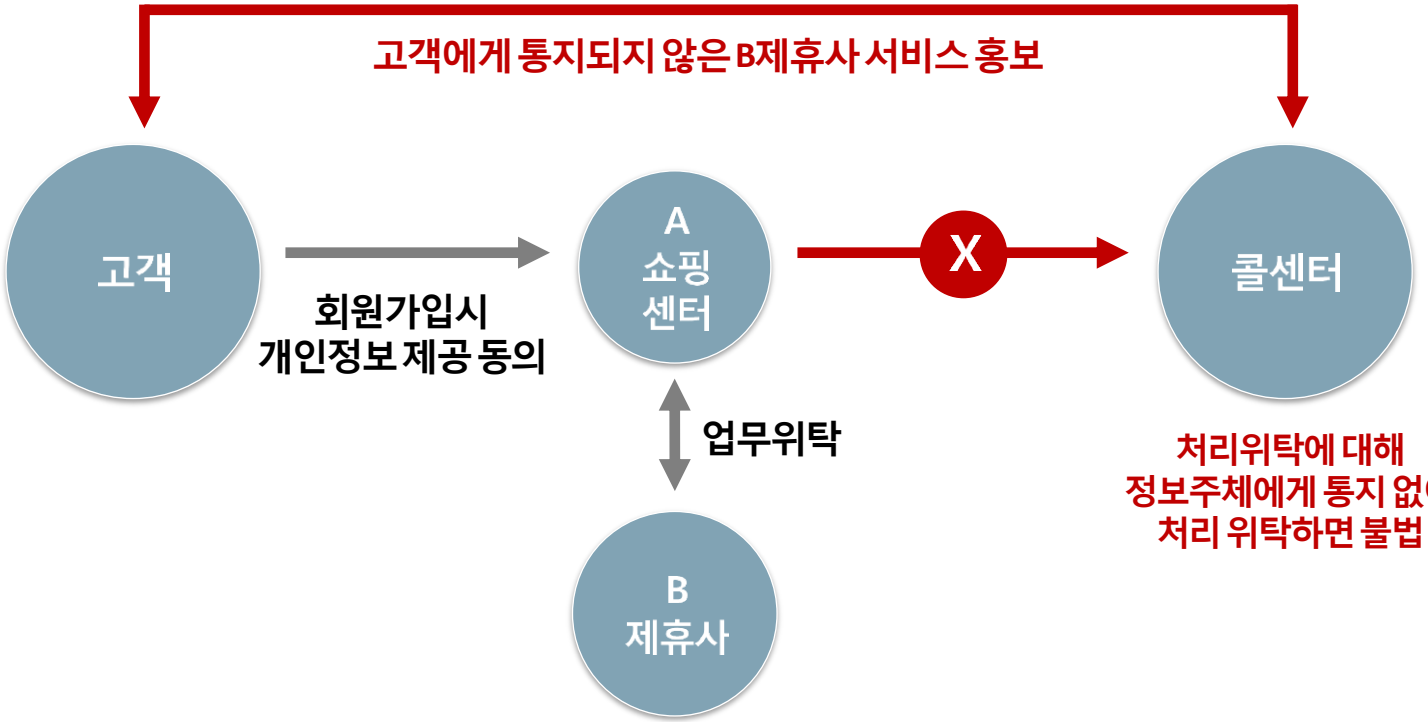
- 해당 사항을 인터넷 홈페이지에 30일 이상 게재
- 인터넷 홈페이지가 없는 경우 사업장 등의 보기 쉬운 장소에 30일 이상 게시

별도 통지 위반 사례

홍보목적의 개인정보처리 위탁시 미통지

본래의 서비스 제공 계약과는 관계없는 제휴서비스를 홍보하기 위하여,

텔레마케팅 업무를 콜센터에 위탁하면서 개인정보 처리위탁 사실을 고객에게 미통지



수탁자를 교육, 감독

교육의 의무

업무 위탁으로 인해 개인정보 분실 · 도난 · 유출 · 위조 · 변조 · 훼손되지 않도록 교육

감독의 의무

수탁자가 개인정보를 안전하게 처리하는지 감독

- 개인정보처리자로서 준수해야 할 사항을 준수하는지
- 계약서에 포함된 개인정보 처리위탁에 관한 사항을 준수하는지

수탁자 감독(정기 점검) 사항(예시)

유형표시	개인정보보호 체계	안전성 확보조치	기타

유형1	• 1만명 미만의 개인정보 보유 소상공인, 단체, 개인
유형1	• 100만명 미만의 개인정보 보유 중소기업 • 10만명 미만 개인정보 보유 대기업, 중견기업, 공공기관
유형1	• 10만 명 이상의 개인정보 보유 대기업, 중견기업, 공공기관 • 100만 명 이상의 개인정보 보유 중소기업, 단체

수탁자 감독(정기 점검) 사항(예시)

유형표시 | **개인정보보호 체계** | 안전성 확보조치 | 기타

- 내부관리계획의 수립
- 개인정보보호책임자 지정
- 개인정보 처리방침의 수립 및 공개
- 개인정보취급자 지정, 관리
- 개인정보취급자의 개인정보보호 서약서 작성
- 개인정보취급자 및 보호책임자 대한 개인정보보호 교육 계획 수립 및 실시

수탁자 감독(정기 점검) 사항(예시)

유형표시 | 개인정보보호 체계 | **안전성 확보조치** | 기타

- 개인정보처리시스템의 계정은 반드시 필요한 개인에게 **최소한의 권한만을 차등 부여**
  - 개인정보취급자별로 한 개의 계정만을 부여, 취급자간 공유 금지
- **접근통제시스템 적용** - 침입차단시스템, 침입탐지시스템 등
- **개인정보의 암호화 보관**
  – PC 및 모바일 내 고유식별정보 암호화, 전송 및 보조저장장치로 전달 시 암호화
- 개인정보처리시템에 대한 **접속기록 6개월 이상** 안전하게 보관, **반기별 1회** 이상 점검접속 기록의 보관·점검
- **악성프로그램을 방지** - 백신 설치, 자동 업데이트 기능 설정, 윈도 보안 패치
- **관리용 단말기**에 대해 임의조작, 목적외 사용되지 않도록 조치
- **물리적 안전조치** – 개인정보 포함 보조저장매체, 서류는 잠금장치 있는 곳에 보관, 물리적 보관장소에 대한 출입통제 절차 운영
- **재해·재난 대비 안전조치** – 재해 • 재난 대비 위기대응매뉴얼 등 마련, 정기 점검. 개인정보처리시스템에 대한 백업 및 복구
- 개인정보 수집목적 달성, 보유기간 만료 시 **개인정보의 완전 파기**, 파기 확인서

수탁자 감독(정기 점검) 사항(예시)

유형표시 | 개인정보보호 체계 | 안전성 확보조치 | **기타**

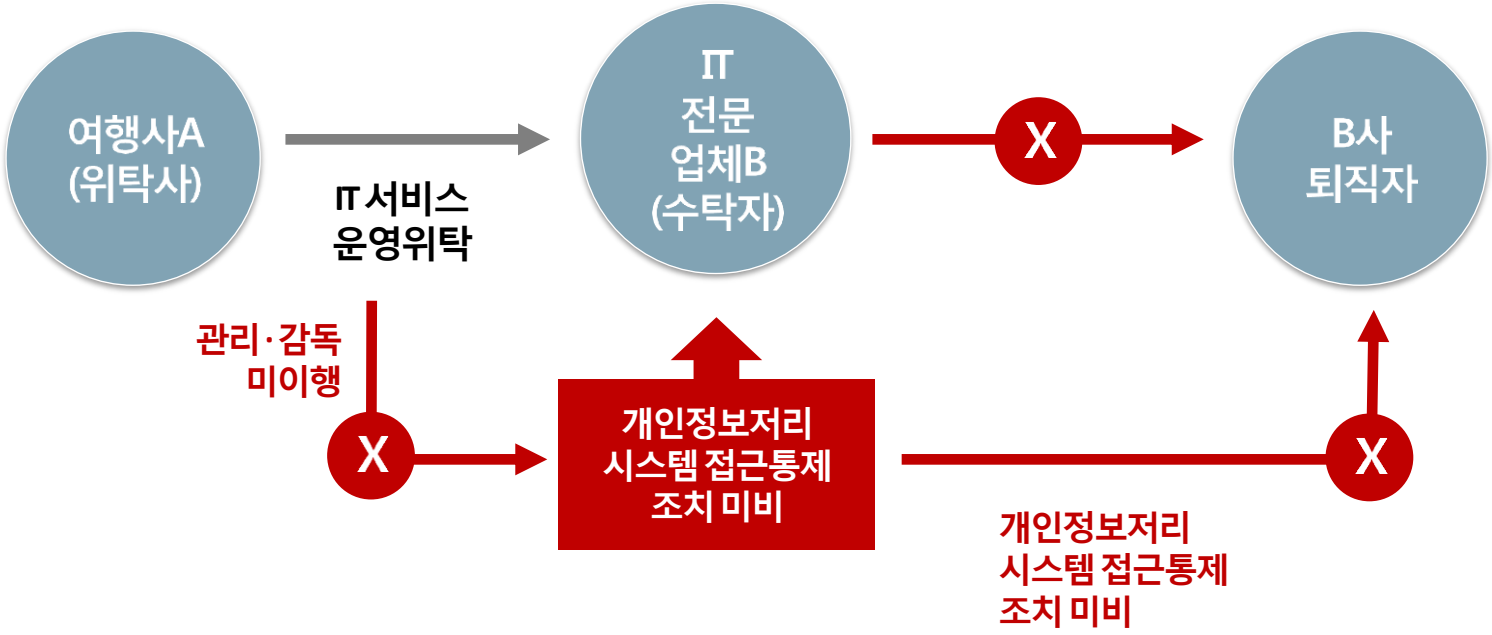
- 재위탁 또는 제3자 제공 금지 준수
- 위탁한 개인정보에 대한 목적 외 이용 금지
- 기타 법령 또는 계약사항 위반 금지
- 개인정보처리 현황 및 실태 파악

수탁자 감독 미비 사례

개인정보처리 수탁자에 대한 관리·감독 위반

IT서비스 운영을 전문업체에 외부 위탁하였으나,

개인정보 처리업무에 대한 관리감독을 수행하지 않아 개인정보 유출



내부 관리계획에 반영

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육
4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지
9. 물리적 안전조치
10. 개인정보 보호조직 구성운영
11. 유출사고 대응계획 수립・시행
12. 위험도 분석 및 대응방안 마련
13. 재해・재난 대비 개인정보처리시스템의 물리적 안전조치
14. 개인정보처리 수탁자의 관리·감독
15. 그밖에 개인정보 보호를 위해 필요한 사항

손해배상책임은 위탁자에게 있음

수탁자의 법 위반으로 발생한 손해배상책임은 위탁자에게 있음
(법 제26조 제6항)
수탁자의 배상책임이 없어진다는 뜻이 아님

수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 법 위반

↓

손해배상책임 발생

↓

수탁자를 개인정보처리자의 소속 직원으로 간주
위탁자 책임

[참고] 개인정보 제3자 제공 vs 위탁

	제 3자 제공 (법 제17조, 제18조)	위탁 (법 제26조)
처리 목적	**제공받는 자**의 이익 / 목적	**제공하는 자**의 이익 / 목적
관리 범위	**제공받는 자**의 책임	**제공하는 자**의 책임
예시	• 경찰에 수사자료로 제공 • 감사기관(수사 수행 목적) 등에 감사자료로 제출 • 마트 이벤트 고객정보를 보험회사 마케팅에 제공	• 민원 처리 만족도 조사를 위해 리서치 업체에 직원 정보 제공 • 직원 교육을 위해 교육 위탁업체에 직원 명단 제공 • SMS를 통한 홍보를 위해 고객의 전화번호를 문자발송 업체에 전달

Ⅲ 수탁자가 준수해야 할 사항

목적 내 이용 및 제3자 제공

위탁 받은 해당 업무 범위를 초과한

개인정보의 이용 또는 제3자 제공 불가

(법 제26조 제5항)

※ 이용・제공한 자와 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 모두 처벌

수탁자에게 적용되는 조항 – 개인정보의 처리

1. 제15조 (개인정보의 수집·이용)
2. 제16조 (개인정보의 수집 제한)
3. 제17조 (개인정보의 제공)
4. 제18조 (개인정보의 목적 외 이용·제공 제한)
5. 제19조 (개인정보를 제공받은 자의 이용·제공 제한)
6. 제20조 (정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)
7. 제21조 (개인정보의 파기)
8. 제22조 (동의를 받는 방법)
9. 제23조 (민감정보의 처리 제한)
10. 제24조 (고유식별정보의 처리 제한)
11. 제24조의2 (주민등록번호 처리의 제한)
12. 제25조(영상정보처리기기의 설치·운영 제한)
13. 제27조(영업양도 등에 따른 개인정보의 이전 제한)
14. 제28조(개인정보취급자에 대한 감독)

수집 업무 수탁자에게 수집 동의 조항 등 적용

대리점에서 개인정보를 수집하여 이동통신사에 넘겨주는 경우,
대리점 역시 수집 이용 동의, 동의 방법, 고유식별 정보 및
민감정보 처리 등에 관한 조항을 적용 받음

정보주체 이외로부터 수집한 개인정보 출처 고지(법 제20조)

- 정보주체의 요구가 있으면 개인정보의 수집 출처, 처리 목적, 처리정지 요구권 있음을 알려줘야 함 (제1항)
- 일정 기준에 해당하는 사업자는 개인정보의 수집 출처, 처리 목적, 처리정지 요구권 있음을 알려줘야 함(제2항)

대상	5만명 이상의 민감정보 또는 고유식별정보. 100만명 이상의 개인정보를 처리하는 자
방법	서면, 전화, 문자전송, 전자우편 등 정보주체가 쉽게 알 수 있는 방법
횟수	- 개인정보를 제공받은 날부터 3개월 이내 -연 2회 이상 주기적으로 개인정보를 받는 경우에는 받은 날부터 연 1회 이상 정보주체에게 알려야 함
고지관련 사실의 관리	정보주체에게 알린 사실, 알린 시기, 알린 방법을 해당 개인정보를 파기할 때까지 보관・관리

수탁자에게 적용되는 조항 – 안전한 관리

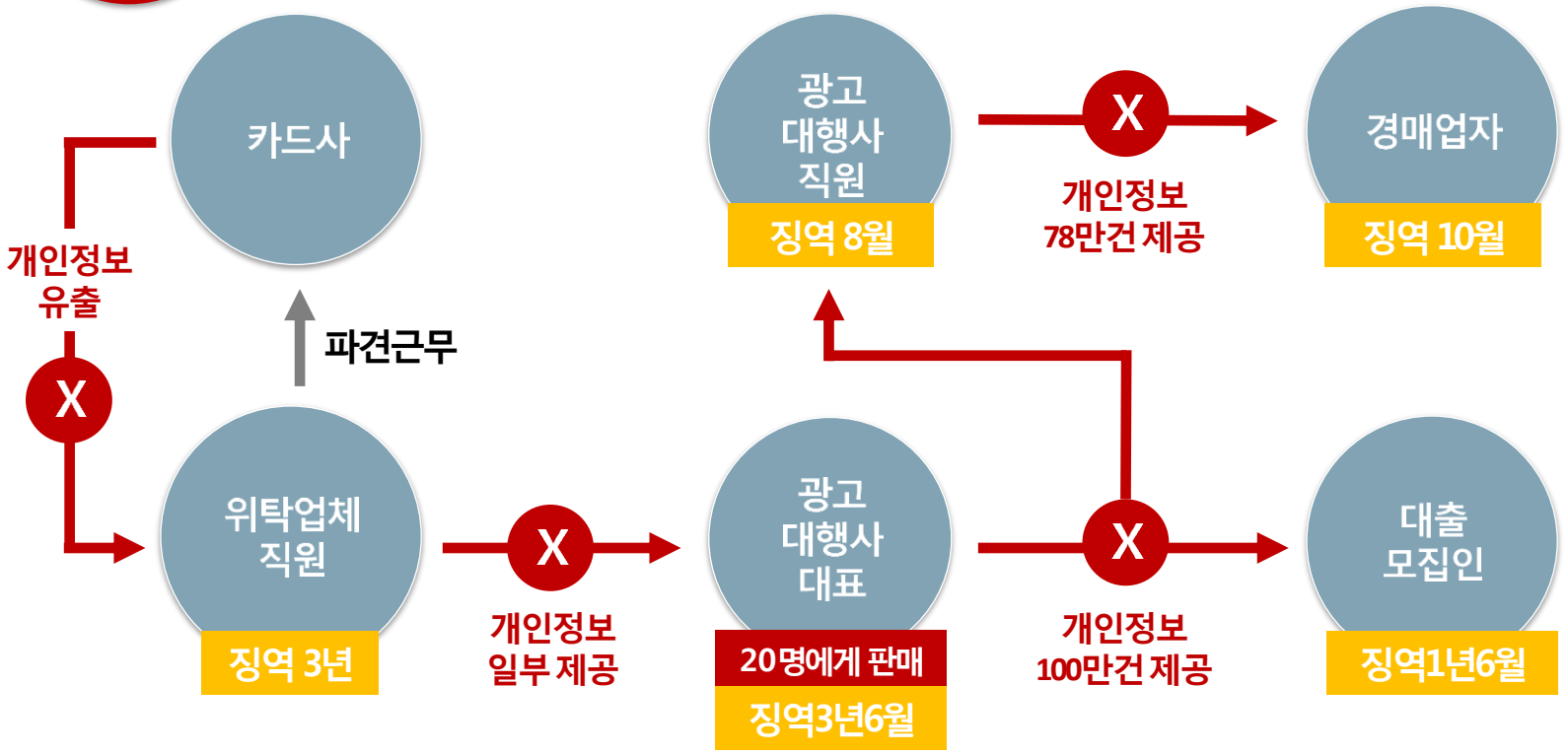
- 제29조(안전조치의무)
- 제30조(개인정보 처리방침의 수립 및 공개)
- 제31조(개인정보 보호책임자의 지정)
- 제33조(개인정보 영향평가)
- 제34조(개인정보 유출 통지 등)
- 제34조의2(과징금의 부과 등)

수탁자에게 안전조치 의무 (제29조)가 있음

- 위탁자의 수탁자 교육, 감독의무(제26조 제4항)도 있음

개인정보 처리위탁업체 인력에 의한 개인정보 유출

카드사에 파견근무를 하며 고객 개인정보 및 사망자 폐업 법인 정보를 USB에 담아 유출



수탁자에게 적용되는 조항 – 정보주체의 권리보장

- 제35조(개인정보의 열람)
- 제36조(개인정보의 정정·삭제)
- 제37조(개인정보의 처리정지 등)
- 제38조(권리행사의 방법 및 절차)

수탁사의 자율 점검(예시) – IT수탁사

분야	점검항목	점검결과		개선기한
		양호	개선필요	
1. 개인정보의 수집·제공	**1. 개인정보 수집에 따른 정보주체의 동의를 받을 때 필수 항목(4개*) 고지 및 내용의 적정성 여부** *필수항목 ①수집의 목적 ②개인정보의 항목 ③개인정보 보유 및 이용 기간 ④동의 거부권 및 거부 시 불이익	O		
	2. 제3자에게 개인정보 제공에 따른 정보주체의 동의를 받을 때 필수항목(5개*) 고지 및 내용의 적정성 여부 *필수항목 ①제공 받는 자 ②이용 목적 ③개인정보의 항목 ④동의 거부권 및 거부 시 불이익		O	20 년 월 일
	3. 고유식별정보, 민감정보, 마케팅용 필요정보 등을 구분하여 동의를 받고 있는지 여부 * 고유식별정보 : 여권번호, 운전면허번호, 외국인등록번호 * 민감정보 : 개인의 과거 및 현재의 병력(病歷), 신체적·정신적 장애, 유전정보, 사상, 정치 등			
2. 주민등록번호 처리제한	**4. 법에 근거하지 않고 주민등록번호를 수집 및 처리하고 있는지 여부**			
	5. 법령에 근거하여 인터넷 홈페이지를 통한 회원가입 시 주민등록번호 외 회원가입 방법(i-PIN, 핸드폰 등) 제공 여부			

IT수탁사 자율점검 목록

분야	점검항목	점검결과		개선기한
		양호	개선필요	
3. 개인정보의 파기	**6. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 영구 삭제하고 있는지 여부**			
	7. 법령에 따라 보존할 경우 다른 개인정보와 분리하여 보관하는지 여부			
4. 업무위탁 계약	**8. 계약문서에 필수 반영사항(7개*)이 포함되었는지 여부** *필수항목 ①위탁업무 수행 목적 외 처리금지 ② 기술·관리적 보호조치 ③ 목적·범위 ④ 재위탁 제한 ⑤접근제한 등 안전조치 ⑥관리·감독사항 ⑦ 손해배상 등 책임에 대한 사항			
5. 개인정보 취급자 감독	**9. 개인정보취급자에 대한 적절한 관리·감독 (접근통제, 보안각서 징구, 교육 등)을 실시하고 있는지 여부**			
6. 개인정보처리 방침의 수립·공개	**10. 개인정보처리방침의 공개 및 필수 항목(10개*) 포함 여부** *필수항목 ①개인정보의 처리 목적 ②처리 및 보유 기간 ③제3자 제공에 관한 사항 (해당 시) ④업무위탁에 관한 사항 (해당 시) ⑤정보주체 권리·의무 및 행사 방법 ⑥개인정보의 항목 ⑦개인정보 파기 ⑧안전성 확보 조치 ⑨처리방침 변경에 관한 사항, ⑩개인정보보호책임자에 관한 사항			

IT수탁사 자율점검 목록

분야		점검항목	점검결과		개선기한
			양호	개선필요	
3. 개인정보의 파기	접근 권한 관리 및 접근통제	11. 시스템에 대한 접근권한 부여시 필요 최소한의 범위로 업무 담당자에 따라(1인 1계정) 차등 부여하는지 여부			
		12. 접근권한의 부여·변경·말소 내역을 기록 및 관리하고, 최소 3년간 보관 하는지 여부			
		13. 안전한 비밀번호 작성규칙을 수립 및 적용 하는지 여부 * 비밀번호 작성 규칙 - (최소 10자리 이상) 영어 대문자, 소문자, 숫자, 특수문자 중 2종류 조합 - (최소 8자리 이상) 영어 대문자, 소문자, 숫자, 특수문자 중 3종류 조합			
		14. 불법적 접근(방화벽) 및 침해사고 방지(침입탐지)를 위한 시스템을 설치 및 운영하고 있는지 여부			
		15. 개인정보취급자가 외부에서 정보통신망을 통한 접속 시 가상사설망(VPN), 전용선 등 안전한 접속수단을 제공하고 있는지 여부			

※ 이하 생략. 전체 내용은 개인정보보호종합지원 포털 참조

Internet On, Security In !

감사합니다