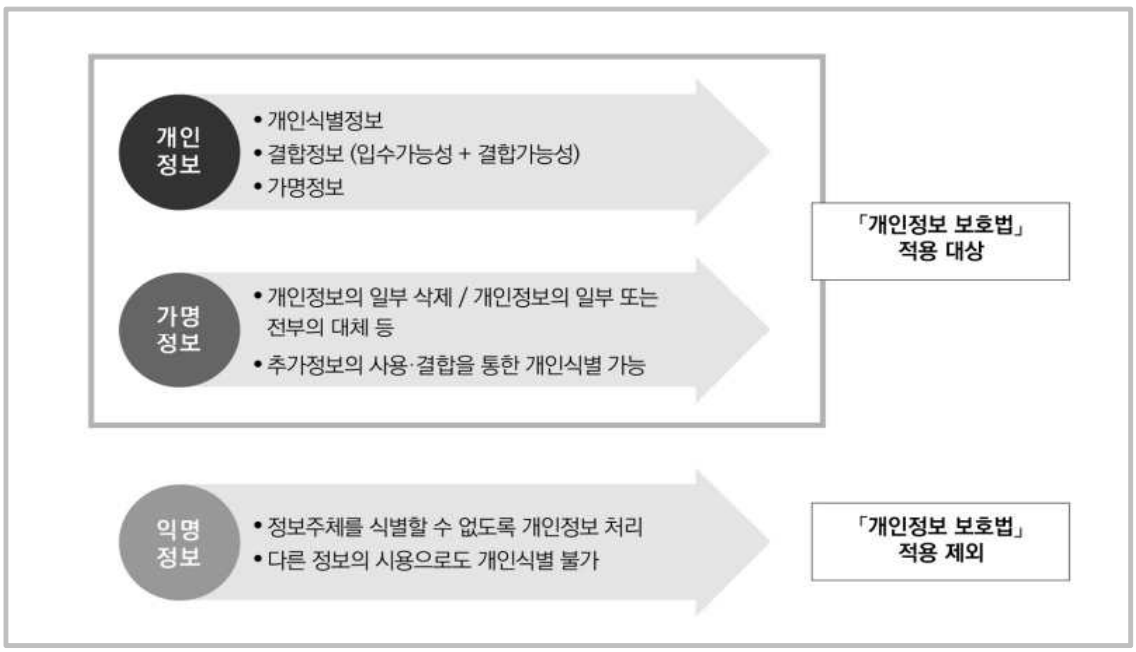
개인정보 보호법 해설

1 개인정보 개요

가. 개인정보의 개념(법 제2조)

- **살아있는 개인에 관한 정보**로서 개인을 알아볼 수 있는 정보
  - 성명, 주민등록번호 및 영상 등을 통하여 개인을 **알아볼 수 있는 정보**
  - 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 **다른 정보와 쉽게 결합**하여 알아볼 수 정보
  - 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(**가명정보**)
- **개인정보·가명정보·익명정보의 비교**



- **개인영상정보**
  - 영상정보처리기기에 의하여 촬영·처리되는 영상정보 가운데 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 "개인영상정보"는 개인정보에 해당함. 따라서 CCTV 및 네트워크 카메라 이외의 카메라, 휴대전화, 블랙박스 등 영상정보처리기기에 의하여 촬영·처리되는 개인의 초상, 행동 등과 관련된 영상으로 해당 개인을 식별할 수 있는 영상정보는 "개인영상정보"에 해당하지는 않지만, 개인정보로서 보호됨.

나. 개인정보의 처리, 정보주체, 개인정보처리자의 개념(법 제2조)

■ 처리

- 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말함
- 다른 개인정보처리자가 처리하고 있거나 처리한 개인정보를 단순히 전달, 전송, 확인 또는 통과만 시켜주는 행위는 처리에 해당하지 않음
- 개인정보 처리 단계

수집·이용	• 수집·이용 (법 제15조) • 최소수집 (법 제16조) • 동의 (법 제22조) ※ 만14세 미만 법정대리인 • 처리제한: 민감정보(법 제23조), 고유식별정보(법 제24조), 주민등록번호(법 제24조의2)
제공·위탁	• 제3자 제공 (법 제17조) • 목적외 이용·제공 제한 (법 제18조) • 처리위탁 (법 제26조)
관리	• 안전조치 의무 (법 제29조) • 개인정보 처리방침 (법 제30조) • 개인정보 보호책임자 (법 제31조) • 개인정보 파일 등록 (법 제32조) • 개인정보 유출 통지·신고 (법 제34조)
파기	• 개인정보의 파기 (법 제21조)

■ 정보주체

- 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말함. 그러므로 법인이나 단체는 정보주체에 해당하지 않음.

  ※ 다만, 법인 또는 단체에 관한 정보이면서 동시에 개인을 식별할 수 있는 정보(대표자 또는 임직원의 이름, 자택주소, 사진 등)나 개인사업자의 상호명, 사업장 주소, 전화번호, 사업자 등록번호 등 개인사업자정보는 각각의 상황이나 맥락에 따라 개인정보 여부를 결정할 수 있고, 개인정보에 해당하는 경우에는 정보주체로 인정할 수 있음

■ 개인정보처리자

- **업무를 목적으로** 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 **공공기관**, 법인, 단체 및 개인 등을 말함.

다. 개인정보 보호의 원칙(법 제3조)

■ 명확한 목적으로 적법하고 정당하게 최소 수집

■ 처리 목적 내에서 적합하게 처리, 목적 외 활용 금지

■ 처리 목적 내에서 정확성·완전성·최신성 보장

■ 정보주체의 권리침해 가능성 등을 고려하여 안전하게 관리

■ 개인정보 처리사항 공개 및 열람청구권 등 정보주체의 권리보장

■ 정보주체의 사생활 침해 최소화 방법으로 처리

■ 익명처리가 가능한 경우에는 익명으로, 익명처리로 목적을 달성할 수 없는 경우에는 가명으로 처리

■ 개인정보처리자의 책임과 의무 준수, 정보주체의 신뢰성 확보

2 개인정보 수집·이용(법 제15조)

가. 동의 없이 처리할 수 있는 개인정보와 동의가 필요한 개인정보를 구분

1) 정보주체의 동의 없이 처리할 수 있는 경우

- 법률에 특별한 규정이 있거나 법령상 의무 준수
- 공공기관이 법령 등에서 정하는 소관업무 수행
- 정보주체와의 계약 체결 및 이행
- 급박한 생명, 신체, 재산의 이익 보호
- 개인정보처리자의 정당한 이익 달성

2) 정보주체의 동의가 필요하여 동의를 받는 경우 *"최소한으로 적법하게"*

- 필수/선택 항목을 엄격하게 구분하여 수집
- 목적에 필요한 최소한의 개인정보 수집\

※ 동의 받을 때 의무 고지사항

- 수집·이용 목적
- 수집 항목
- 보유·이용 기간
- 동의 거부 권리 및 동의 거부 시 불이익 내용

☞ 동의 의무사항 미고지 시 3천만 원, 수집 위반 시 5천만 원 이하 과태료

나. 개인정보 동의 받는 방법(법 제22조)

1) 동의서에 특히 명확히 표시해야 하는 항목(시행령 제17조)

- 재화나 서비스의 홍보 및 판매 연락을 할 수 있다는 사실
- 민감정보, 고유식별번호(여권번호, 운전면허번호, 외국인등록번호)
- 개인정보의 보유 및 이용 기간
- 개인정보 제공받는 자 및 제공받는 자의 이용 목적

※ 중요사항 명확하게 표시 방법

- 글씨는 9포인트 이상으로 하되 다른 내용보다 20% 이상 크게
- 다른 색의 글씨, 굵은 글씨 또는 밑줄 등 사용하여 명확히 드러나게
- 중요한 내용이 많은 경우는 별도 요약 제시

☞ 위반 시 1천만 원 이하 과태료

2) 구체적으로 각각, 별도 동의

① 수집·이용 동의(제15조 제1항제1호) ② 제3자 제공 동의(제17조 제1항1호) ③ 국외 제3자 제공 동의(제17조 3항) ④ 마케팅 목적 처리 동의(제 22조 제3항) ⑤ 법정대리인의 동의(제22조 제5항)	⑥ 목적 외 이용 · 제공 동의(제18조 제2항제1호) ⑦ 개인정보를 제공받는 자의 이용 · 제공 제한(제19조 제1호) ⑧ 민감정보 처리 동의(제23조 제1항제1호) ⑨ 고유식별정보 처리 동의(제24조제1항제1호)

다. 민감정보 및 고유식별번호 처리 제한(법 제23조, 제24조)

1) 원칙적으로는 처리 금지

2) 처리 가능한 경우

- 별도 동의 얻은 경우
- 법령에서 처리를 요구하거나 허용한 경우

☞ 위반 시 5년 이하의 징역 또는 5천만 원 이하의 벌금

민감정보	고유식별정보
- 사상, 신념 - 노동조합·정당의 가입 및 탈퇴, 정치적 견해 - 건강, 성생활 등의 정보, 유전정보 - 범죄경력(전과·수형기록등) - 개인의 신체적, 생리적, 행동적 특징에 관한 정보 - 인종이나 민족에 관한 정보	- 주민등록번호 *(동의 받아도 처리 불가)* - 운전면허번호 - 여권번호 - 외국인등록번호

분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 않도록 암호화 등 안전성 확보 조치

라. 주민등록번호 처리의 제한(법 제24조의2)

1) 동의 받아도 주민등록번호 처리 불가

2) 처리 가능한 경우

- 법률, 시행령에 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
- 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위해 명백히 필요하다고 인정되는 경우
- 위에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

☞ 위반 시 3천만 원 이하의 과태료

마. 영상정보처리기기의 운영·관리

1) 영상정보처리기기 운영·관리 방침 수립 및 홈페이지에 공개

2) 다음 사항이 포함된 안내판 설치

- 설치 목적 및 장소
- 촬영 범위 및 시간
- 관리책임자의 성명(직책) 및 연락처 기재

3) 개인영상정보 관리대장 기록·관리

3 개인정보 제공·위탁

가. 개인정보 업무위탁과 제3자 제공의 비교

구분	개인정보처리위탁	제3자 제공
관련조항	법 제26조	법 제17조, 제18조
이전목적	제공하는 자의 이익/목적	제공받는 자의 이익
예측 가능성	정보주체가 사전 예측 가능	정보주체가 사전 예측 곤란
이전 방법	위탁사실 홈페이지에 공개 ☞ 정보주체에게 위탁에 대한 동의 불필요 ☞ 마케팅(홍보 등) 위탁사실은 서면, 문자전송 등으로 정보주체에게 통지	제공목적 등 고지 후 정보주체의 동의 획득
관리·감독의무	위탁자(수탁자를 직원으로 간주)	제공받는 자
손해배상책임	위탁자 부담	제공받는 자 부담
이행사항	① 위탁계약서 작성(필수항목 7가지 포함) ☞ 표준 개인정보처리위탁계약서 참고 ② 위탁업무 내용 및 수탁자 정보 홈페이지(개인정보 처리방침 등) 공개 ③ 수탁자에 대한 교육 실시 및 개인정보 안전조치 사항 등 관리·감독 ④ 업무 종료 시 수탁자의 개인정보 파기(반환) 여부 확인(증빙자료) 및 보안확약서 징구	① 정보주체로부터 동의를 받는 경우에는 5가지 항목을 고지하고 동의를 획득 ② 법률 등에 의해 개인정보를 목적 외로 제3자에게 제공하는 경우(법 제18조) - 개인정보 보호책임자의 승인을 받아 제공받는 자에게 문서로 이용 제한 및 보호조치 요청 - [개인정보의 목적 외 이용 및 제3자 제공 대장] 기록·관리 - 제공한 날부터 30일 이내 제공 현황을 홈페이지에 공개(10일 이상 게재) ※ 정보주체 동의, 수사 목적인 경우 공개 제외
예시	• PC, 홈페이지 유지관리 • 방과후 교육을 외부업체에 위탁 • 졸업앨범, 학생증 제작 • 직원 교육을 위해 위탁업체에 직원 명단 제공 • 사설알림서비스 (학교에서 일괄 수집하여 운영하는 경우)	• 경찰에 수사자료 제공 • 법원의 재판업무 수행 • 감사기관 등에 감사자료로 제출 • 마케팅 회사에 제공

(참고)

현장체험 학습 진행 시 개인정보 이용·제공	
방법 1) 여행사 계약	**방법 2) 학교 자체 추진**
▶ **개인정보 처리 위탁** ① **[사업 시작]** 표준 개인정보처리 위탁계약서 체결 ② **[사업 중]** 수탁자 관리·감독 ☞ 수탁자교육 증빙자료 징구 ③ **[사업 종료]** 개인정보 파기 확인서 징구 ④ 학교 홈페이지 등에 위탁업무 내용 지속적으로 게시	▶ **학교에서 업무처리** ▶ **보험가입 시, 제3자 제공** ① 제3자 제공 동의서 필요 ② 개인정보 안전조치 후, 제3자에게 제공

나. 개인정보의 제공(법 제17조)

1) 정보주체의 동의를 받지 않는 경우

- 법률에 특별한 규정이 있거나 법령상 의무 준수
- 공공기관이 법령 등에서 정하는 소관업무 수행
- 급박한 생명, 신체, 재산의 이익 보호

2) 정보주체의 동의를 받는 경우

※ 동의 받을 때 의무 고지사항

- 개인정보를 **제공받는 자**
- 제공받는 자의 개인정보 **이용 목적**
- 제공하는 개인정보 **항목**
- 제공받는 자의 개인정보 **보유 및 이용 기간**
- 동의 거부 **권리 및** 동의 거부 시 **불이익 내용**

☞ 위반시 5년 이하의 징역 또는 5천만 원 이하의 벌금

다. 개인정보 제공 범위 확대(법 제17조 4항)

1) 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체의 동의 없이 이용 가능

- 당초 수집 목적과 관련성이 있는지 여부
- 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부 등
- 정보주체의 이익을 부당하게 침해하는지 여부
- 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

2) 위 고려사항에 대한 판단 기준을 개인정보 처리방침에 미리 공개해야함

라. 개인정보의 목적 외 이용·제공(법 제18조)

1) **원칙적으로 금지**, 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는 경우 예외적으로 허용

2) 정보주체의 동의를 받지 않는 경우

- 법률에 특별한 규정이 있거나 법령상 의무 준수
- 제3자의 급박한 생명, 신체, 재산의 이익 보호

〈아래의 경우는 공공기관만 해당〉

- 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로 개인정보보호 위원회 심의·의결을 거친 경우
- 조약, 그 밖의 국제 협정의 이행을 위하여 외국 정부 또는 국제기구에 제공
- 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
- 법원의 재판 업무 수행을 위하여 필요한 경우
- 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

☞ 위반 시 5년 이하의 징역 또는 5천만 원 이하의 벌금

3) 정보주체의 동의를 받는 경우

※ 동의 받을 때 의무 고지사항

- 개인정보를 제공받는 자
- 제공받는 자의 개인정보 이용 목적
- 제공하는 개인정보 항목
- 제공받는 자의 개인정보 보유 및 이용 기간
- 동의 거부 권리 및 동의 거부 시 불이익 내용

4) 목적외 이용·제공 시 이행사항

▪ 제공 받는 자에게 이용목적, 이용방법 그 외 필요사항에 대한 제한 및 개인정보 **안전성 확보조치 마련을 공문으로 요청**

요청자 (제공 받는 자)		제공자
개인정보 제공 요청 (공문)	❶	• 요청 자료를 공문으로 제공 • 개인정보 안전성 확보 조치 요청 (개인정보 이용목적, 방법, 그 외 필요사항 등)
	❷	
안전성 확보조치 이행 및 결과를 공문으로 회신	❸	• 목적 외 이용 및 제3자 제공 대장 작성 • 홈페이지에 공개 - 제공 날짜, 법적 근거, 목적, 개인정보의 항목 - 제공일로 부터 30일 이내 10일 이상

▪ **이용·제공 내역을** 30일 이내, 10일 이상 **인터넷 홈페이지에 게재**

- 게재항목: 이용한 날짜, 법적근거, 목적, 개인정보의 항목
- 홈페이지 게재 제외: 정보주체 동의, 범죄수사와 공소의 제기 및 유지를 위하여 제공한 경우

▪ 개인정보 목적 외 이용 및 제3자 제공 대장 기록

〈목적외 이용 및 제3자 제공 대장 서식〉

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ]목적외 이용	[ ]목적외 제3자 제공	
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속 성 명 전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명 소 속 전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

마. 개인정보 위탁(법 제26조)

〈업무 위탁 예시〉

- 개인정보가 포함된 자료의 출력을 출판사·인쇄소에 맡기는 경우
- 학생증·졸업앨범 등의 외주 제작, 방과후 교육을 외부업체에 위탁
- 졸업여행, 현장학습 등 여행사를 통한 보험 가입
- 외부업체의 홈페이지 웹호스팅, PC 유지관리 등

1) 개인정보 위탁 시 단계별 이행사항

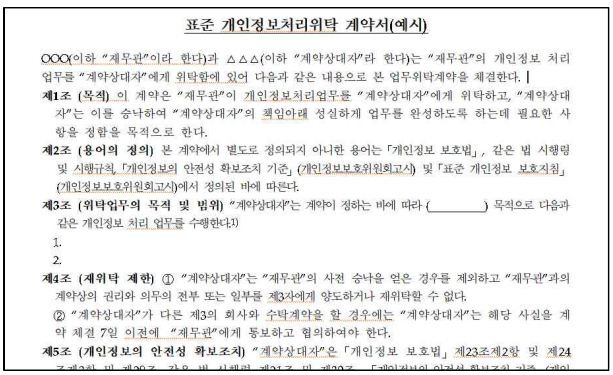
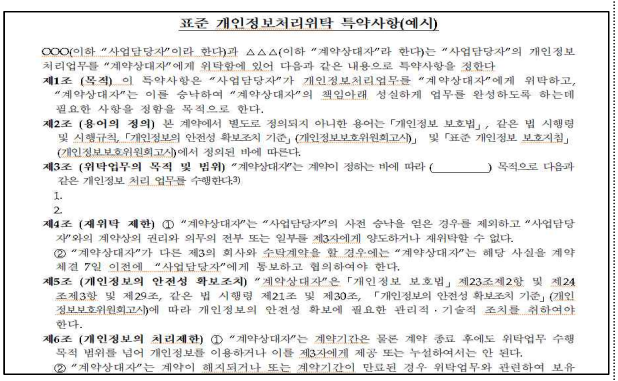
구분	이행사항
계약 전	• 위탁할 업무 범위 구분 → 수탁자 선정 → 처리범위의 명확화 • 개인정보 처리위탁 문서 작성 (표준 개인정보처리 위탁 계약서 또는 특약사항)
계약 후	• 홈페이지 개인정보처리방침에 위탁에 관한 사항 공개 (위탁업무 내용, 수탁자 정보) • 수탁자 교육: 교육 계획 수립 → 이행* → 결과 보고 * 위탁자 및 제3자 전문가의 집합·온라인 교육, 수탁자의 자체 교육 모두 가능 • 수탁자 안전조치의무 준수 여부 등 점검 : 점검 계획 수립 → 이행** → 결과 보고 ** 자료제출 요구, 현장방문, 원격점검 등 다양한 수단 활용 가능
계약 종료 후	• 수탁자의 개인정보 파기(반환)을 통한 개인정보 불법 처리 유통 방지 - 수탁자는 위탁자 요청 시 즉시 반환하며, 개인정보의 무결성 및 완전성 보장 - 위탁자는 수탁자의 개인정보 파기 여부 확인 후 개인정보 파기 확인서 징구

2) 위탁 계약서 필수 기재 사항 *☞ 부록의 표준 개인정보처리 위탁 계약서(예시) 참고*

- 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 기술적·관리적 보호조치에 관한 사항
- 위탁업무의 목적 및 범위
- 재위탁제한에 관한 사항
- 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
- 위탁업무와 관련하여 보유하고 있는 개인정보의 관리·감독에 관한 사항
- 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

☞ 손해배상책임 발생 시, 수탁자는 개인정보처리자의 소속직원으로 간주

〈개인정보처리 위탁 계약서 예시〉

표준 개인정보처리위탁 계약서	표준 개인정보처리위탁 특약사항
	

표준 개인정보처리위탁 계약서(예시)

OOO(이하 "제무관"이라 한다)과 △△△(이하 "계약상대자"라 한다)는 "제무관"의 개인정보 처리 업무를 "계약상대자"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "제무관"이 개인정보처리업무를 "계약상대자"에게 위탁하고, "계약상대자"는 이를 승낙하여 "계약상대자"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」(개인정보보호위원회고시) 및 「표준 개인정보 보호지침」(개인정보보호위원회고시)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "계약상대자"는 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.)

1.
2.

제4조 (재위탁 제한) ① "계약상대자"는 "제무관"의 사전 승낙을 얻은 경우를 제외하고 "제무관"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "계약상대자"가 다른 제3의 회사와 수탁계약을 할 경우에는 "계약상대자"는 해당 사실을 계약 체결 7일 이전에 "제무관"에게 통보하고 협의하여야 한다.

제5조 (개인정보의 안전성 확보조치) "계약상대자"은 「개인정보 보호법」 제23조제2항 및 제24

표준 개인정보처리위탁 특약사항(예시)

OOO(이하 "사업담당자"이라 한다)과 △△△(이하 "계약상대자"라 한다)는 "사업담당자"의 개인정보 처리업무를 "계약상대자"에게 위탁함에 있어 다음과 같은 내용으로 특약사항을 정한다

제1조 (목적) 이 특약사항은 "사업담당자"가 개인정보처리업무를 "계약상대자"에게 위탁하고, "계약상대자"는 이를 승낙하여 "계약상대자"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」(개인정보보호위원회고시), 및 「표준 개인정보 보호지침」(개인정보보호위원회고시)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "계약상대자"는 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.)

1.
2.

제4조 (재위탁 제한) ① "계약상대자"는 "사업담당자"의 사전 승낙을 얻은 경우를 제외하고 "사업담당자"와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "계약상대자"가 다른 제3의 회사와 수탁계약을 할 경우에는 "계약상대자"는 해당 사실을 계약 체결 7일 이전에 "사업담당자"에게 통보하고 협의하여야 한다.

제5조 (개인정보의 안전성 확보조치) "계약상대자"은 「개인정보 보호법」 제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "계약상대자"는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "계약상대자"는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유

4 개인정보 파기

가. 개인정보의 파기(법 제21조)

1) 보유기간 경과, 목적 달성 등 **지체 없이(5일 이내)** 파기. 다만, 다른 법령에 따라 보존하여야 하는 경우는 보존
2) 개인정보 파기 시 복구 또는 재생되지 않도록 조치
3) 다른 법령에 따라 보존하여야 하는 경우 다른 개인정보와 분리하여 저장·관리
4) 개인정보처리자는 개인정보파일의 파기에 관한 사항을 기록 관리하고 반드시 개인정보 보호책임자는 파기 결과 확인

나. 파기방법

구분	전부 파기	일부 파기
전자적 파일 (하드디스크, USB 등)	매체를 파괴하여 복구할 수 없도록 조치 또는 전용 소자장비를 이용하여 삭제 ※ 컴퓨터 등의 불용처분 및 매각 시 데이터 완전 삭제	개인정보 삭제 후 복구·재생되지 않도록 관리 감독
기록물, 인쇄물, 서면, 기록매체 등	분쇄 또는 소각	해당 부분을 마스킹 또는 천공 등으로 삭제

다. 학교에서의 개인정보 파기

- **대상**: 학기 초, 학기 중 수집한 각종 개인정보, 학생기초 자료조사서, 홈페이지 회원정보 등
- **절차**

파기 계획 수립	⇨	파기 수행	⇨	파기 완료 보고
내부결재, 책임자 승인		담당자 파기 또는 개인정보보호 담당자 수합 또는 부서별 파기 등		내부결재, 책임자 승인

- 각급학교 표준개인정보파일 중 “홈페이지 회원정보”는 추가로 「개인정보파일 파기관리 대장」에 기록(파기사유: 회원정보 부분파기)

※ 부록의 개인정보 파기 계획 및 결과 보고(예시) 참조

5 개인정보의 안전한 관리

가. 안전조치의무(법 제29조)

1) 개인정보가 분실,도난,유출,위조,변조,훼손되지 않도록 안전성 확보 조치 필수

관리적 안전조치	기술적 안전조치	물리적 안전조치
- 내부관리계획 수립 및 시행 - 내부관리계획 이행실태점검	- 접근권한의 관리 - 비밀번호의 관리 - 접근통제 시스템 설치 및 운영 - 개인정보의 암호화 - 접속기록의 보관 및 위·변조 방지 - 보안프로그램 설치 및 운영	- 물리적 접근방지 (보관시설 마련, 잠금장치 설치 등) - 개인정보의 파기

2) 내부관리계획 수립 및 시행

- 필수적 내용을 포함하여 수립 (학교용 예시 참고)
- 개인정보 보호책임자 결재 및 내부직원(계약직 포함) 전파(공람, 교육 등)
- 연1회 이상 내부 관리계획 이행실태 점검 실시 (이행실태 점검표 참조)

※ 내부관리계획에 포함되어야 할 내용

- 개인정보 보호책임자의 지정에 관한 사항
- 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
- 개인정보취급자에 대한 교육에 관한 사항
- 접근 권한의 관리에 관한 사항
- 접근 통제에 관한 사항
- 개인정보의 암호화 조치에 관한 사항
- 접속기록 보관 및 점검에 관한 사항
- 악성프로그램 등 방지에 관한 사항
- 물리적 안전조치에 관한 사항
- 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
- 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
- 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
- 그 밖에 개인정보 보호를 위하여 필요한 사항
  - 개인정보의 목적 외 이용 및 제3자 제공 절차에 관한 사항
  - 개인정보의 파기 절차에 관한 사항

3) 개인정보취급자 관리·감독

- 개인정보 취급자(교직원) 대상 교육 실시

  ☞ 개인정보보호 교육 계획의 수립(내부 관리계획에 포함하여 수립 가능)

  - 교육목적, 교육대상, 교육내용, 교육일정, 교육방법 등의 내용 포함
  - 교육이수 증빙자료(사진, 출석부, 이수증 등) 보관
- 개인정보 취급자의 개인정보 처리범위를 업무상 필요한 한도 내 최소한으로 제한

4) 접근 권한의 관리

- 개인정보처리시스템 권한부여, 변경, 말소에 대한 내역을 대장으로 관리
- 전자적으로 기록하거나 수기대장으로 관리(최소 3년 보관)

  ☞ 나이스, K-에듀파인: 권한 관리 메뉴 활용, 홈페이지: 관리 메뉴 없는 경우 별도 대장 관리
- 사용자 계정은 개인정보취급자별로 발급, 다른 개인정보취급자와 공유되지 않도록 조치

5) 접근 통제

- 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음의 기능을 포함한 조치
  - 개인정보처리시스템에 대한 접속권한을 IP·MAC주소 등으로 제한하여 인가받지 않은 접근 제한
  - 개인정보처리시스템에 접속한 IP·MAC주소 등을 분석하여 불법적 개인정보 유출시도 탐지 및 대응
- 외부에서 개인정보처리시스템 접속 시 가상사설망(VPN) 또는 전용선 등 안전한 접속수단 및 인증수단 적용
- 개인정보취급자가 일정시간 이상 업무를 처리하지 않는 경우 자동으로 시스템 접속 차단 조치
- 업무용 모바일 기기의 분실, 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 조치

6) 개인정보의 암호화

- 내부망(업무용 PC등)에 고유식별정보(주민등록번호 등) 저장하는 경우 암호화하여 저장
- 고유식별정보, 비밀번호, 생체인식정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달할 경우 암호화 처리

※ PC 내 개인정보 파일 정비 및 중요 데이터 암호화

- 자체점검: 매월 세 번째 수요일(사이버 보안 진단의 날)
- 개별 점검 후 파일 삭제 또는 암호화 처리 **※ 주민등록번호 포함 파일은 암호화가 의무**
- 개인정보파일 **암호화 미조치 파일이 있는 경우** 메시지 발생 ☞ 즉시 처리

대상파일	처리방법	비고
고유식별번호 (주민등록번호 등) 포함된 파일	법령근거 없다면 ☞ **삭제** 또는 생년월일로 대체 법령근거 있다면 ☞ 개인정보관리프로그램 **암호화**() **또는** 개별 프로그램 파일 암호화	보유 기간 종료 또는 이용 목적이 달성된 경우 즉시(5일 이내) **삭제**
개인정보 포함 파일, 중요자료 파일 등	**개별프로그램 파일 암호화** ☞ **한글**-저장하기-문서암호 설정 ☞ **엑셀**-저장하기-도구:일반옵션-암호 설정 ※ 프로그램 버전에 따라 설정방법은 다를 수 있음	

7) 접속기록의 보관 및 점검

- 개인정보처리시스템에 대한 접속기록은 최소 1년 이상 보관·관리
- 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우 2년 이상 보관·관리
- 접속기록 항목: (누가)접속자 ID, (언제)접속일시, (어디에서)접속자 IP주소, (어떤정보 대상으로)처리한 정보주체 정보, (무엇을 했는가)수행업무(열람·수정·인쇄·입력 등)
- 개인정보처리시스템의 접속기록 등은 월 1회 이상 점검

8) 악성프로그램 등 방지

- 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영
  - 보안 프로그램의 자동업데이트 기능 사용 또는 일 1회 이상 업데이트를 실시하여 최신의 상태 유지
  - 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안업데이트 공지가 있는 경우 즉시 업데이트 실시
  - 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

9) 관리용 단말기의 안전조치

- 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음의 안전조치 이행
  - 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
  - 본래 목적 외로 사용되지 않도록 조치
  - 악성프로그램 감염 방지 등을 위한 보안조치 적용

10) 물리적 안전조치

- 전산실 및 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우, 이에 대한 출입통제 절차를 수립·운영
- 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관
- 개인정보가 포함된 보조저장매체의 반·출입 통제를 위한 보안대책 마련

※ 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우, 이를 적용하지 아니할 수 있음

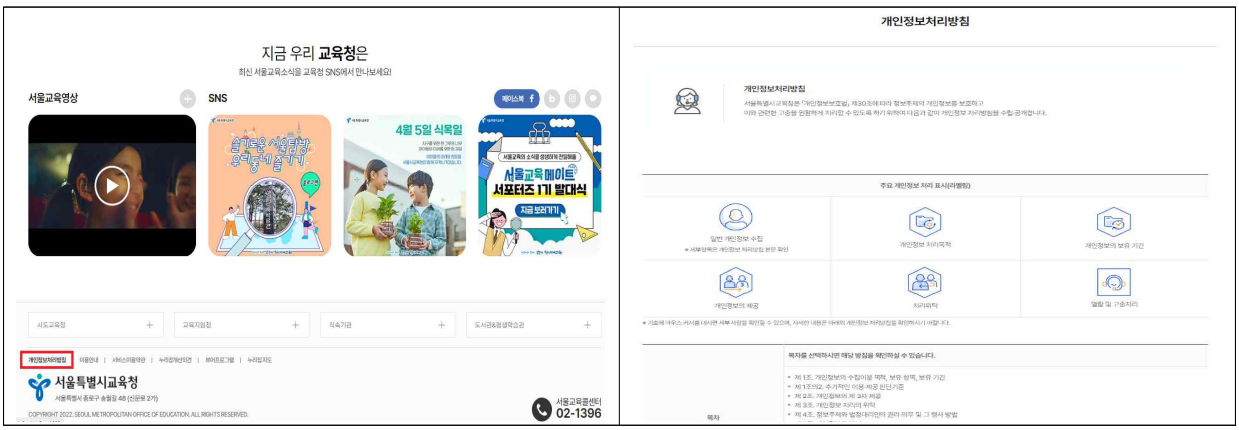
나. 개인정보 처리방침의 수립 및 공개(법 제30조)

- 개인정보 처리방침의 필수항목이 누락되지 않도록 수립
- 개인정보 처리방침 공개 및 변경 이력 관리
- 개인정보보호종합지원시스템(https://intra.privacy.go.kr)에 개인정보파일 현행화
- 처리방침의 개인정보파일과 개인정보보호종합지원시스템 개인정보파일 목록 일치
- 학교 개인정보 처리방침(작성예시) 참고

※ 개인정보 처리방침 주요 내용

- 개인정보의 처리 목적
- 처리하는 개인정보의 항목
- 개인정보의 처리 및 보유 기간
- 개인정보의 제3자 제공에 관한 사항(해당되는 경우)
- 개인정보의 파기에 관한 사항
- 개인정보 처리 개인정보처리 위탁에 관한 사항(해당하는 경우)
- 개인정보의 추가적인 이용·제공의 기준(해당하는 경우)
- 가명정보 처리에 관한 사항(해당하는 경우)
- 개인정보의 안전성 확보 조치에 관한 사항
- 정보주체와 법정대리인의 권리·의무 및 그 행사 방법
- 개인정보 처리방침의 변경에 관한 사항
- 개인정보 보호 책임자의 성명, 업무 담당 부서의 명칭과 연락처
- 개인정보의 열람청구를 접수·처리하는 부서
- 정보주체의 권익침해에 대한 구제방법
- 홈페이지 접속 시 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항 (해당하는 경우)

〈개인정보 처리방침 메뉴 위치 및 방침 예시〉



다. 개인정보 보호책임자의 지정(법 제31조)

1) 개인정보 보호책임자(CPO): 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자(각급학교장)

2) 개인정보보호 책임자 주요 역할 및 의무

- 개인정보 보호 계획의 수립 및 시행
- 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- 개인정보 처리와 관련한 불만의 처리 및 피해 구제
- 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
- 개인정보 보호 교육 계획의 수립 및 시행
- 개인정보파일의 보호 및 관리·감독

- 개인정보 처리방침의 수립·변경 및 시행
- 개인정보 보호 관련 자료의 관리
- 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

라. 개인정보파일의 등록 및 공개(법 제32조)

1) 각급학교 개인정보파일 표준목록(8종)을 개인정보보호종합지원시스템에 등록·현행화

2) 개인정보보호종합지원시스템에 등록된 개인정보파일 표준목록(8종)과 학교홈페이지 개인정보 처리방침에 공개된 파일목록 일치

※ 각급학교 개인정보파일 표준목록(8종): 상세내역은 부록 참조
① 학교생활기록부 ② 학부모서비스 신청자 명단 ③ 학생건강기록부 ④ 발전기금접수대장
⑤ ○○홈페이지 회원정보 ⑥ 민원처리부 ⑦ 학교운영위원회 명부 ⑧ 스쿨뱅킹(CMS) 정보

3) 개인정보파일 정비 방법

- 정비 시기: 교육청에서 정비 공문 안내 시 실시(4~5월 예정)
- 접속 주소: 개인정보보호종합지원시스템(https://intra.privacy.go.kr)
- 처리순서

① 담당자 등록	② 담당자 승인	③ 로그인	④ 개인정보파일 현행화	⑤ 개인정보파일 승인
[학교]	[교육청] - 유·초·중: 교육지원청 - 고·특: 본청 디지털·혁신미래교육과	[학교]	[학교]	[교육청] - 유·초·중: 교육지원청 - 고·특: 본청 디지털·혁신미래교육과

- 기존에 담당자를 등록한 경우에는 ①, ② 생략
- 담당자: 개인정보보호책임자(교장), 개인정보보호총괄관리자(개인정보보호 업무 담당자)
- 학교 개인정보취급자 등록 시엔 학교 담당자가 승인 처리

담당자 등록		승인자
(모든 기관) 개인정보 취급자	▶	소속기관 내 개인정보보호 총괄관리자
유치원·초·중학교 개인정보보호 총괄관리자	▶	교육지원청 개인정보보호 총괄관리자
고등학교 개인정보보호 총괄관리자	▶	서울시교육청 개인정보보호 총괄관리자 [디지털·혁신미래교육과]
교육지원청 개인정보보호 총괄관리자	▶	
직속기관 개인정보보호 총괄관리자	▶	

6 개인정보 유출과 대응방안

가. 개인정보 유·노출 및 침해사고 대응절차 수립: 내부 관리계획에 포함하여 수립

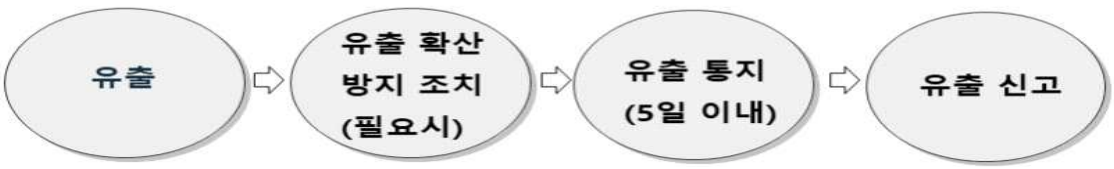
나. 개인정보 유출 통지(법 제34조)

1) 개인정보 유출의 종류(교육부 개인정보 보호지침 제50조)

※ 개인정보의 유출: 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것

- 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
- 데이터베이스 등 개인정보처리시스템에 권한이 없는 자가 접근한 경우
- 권한이 없는 자에게 개인정보가 잘못 전달된 경우

2) 유출 대응 절차



3) 유출 통지 항목

- 유출된 개인정보의 항목
- 유출된 시점과 그 경위
- 정보주체가 피해를 최소화할 수 있는 방안
- 개인정보처리자의 대응조치 및 피해 구제절차
- 피해 발생 시 신고 등을 접수할 수 있는 담당부서 및 연락처

4) 유출 신고(교육부 개인정보 보호지침 제53조)

- 유출 신고 : 1건 이라도 유출시 유출내용 및 조치결과를 5일 이내에 신고
- 신고 방법 : 상급기관에 공문 보고(개인정보 유출신고서 첨부)하고 교육부 '개인정보 유출 신고센터'(https://privacy.moe.go.kr)에 직접 신고

※ 단, 1천명 이상 유출 시 개인정보보호위원회 또는 인터넷진흥원에 추가 신고

다. 홈페이지 개인정보 유출 방지 노력

1) 전 직원 교육을 통한 개인정보유출 방지 교육 실시
2) 게시판 운영목적을 고려한 게시글 공개기한 설정 및 관리
3) 게시글에 개인정보가 포함되지 않도록 작성 주의
4) 첨부자료 중 개인정보가 포함되지 않도록 주의
5) **엑셀파일은 PDF파일로 변환하여 업로드** (숨김으로 개인정보 유출 가능)

7 정보주체의 권리보호

가. 정보주체의 권리 보장

1) 정보주체의 권리(제4조)

- 개인정보의 처리에 관한 정보를 제공받을 권리
- 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
- 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급 포함)을 요구할 권리
- 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
- 개인정보의 처리 피해를 신속하고 공정한 절차에 따라 구제 받을 권리

2) 개인정보의 열람(제35조)

- 정보주체는 자신의 개인정보에 대해 열람 요구가 가능하며, 개인정보처리자는 정당한 사유가 없는 한 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 함
- 다음 중 어느 하나에 해당하는 경우 열람요구를 거절할 수 있고, 그 사유를 지체없이 해당 정보주체에게 알려야 함
  - 법률에 따라 열람이 금지되거나 제한되는 경우
  - 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해 할 우려가 있는 경우
  - 공공기관이 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우

> • 조세의 부과·징수 또는 환급에 관한 업무
> • 초·중등교육법 및 고등교육법에 따른 각급학교, 평생교육법에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
> • 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
> • 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
> • 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

  - 요청일로부터 10일 이내에 열람정보(열람할 개인정보와 열람이 가능한 날짜, 시간 및 장소) 또는 열람 거절 사유 및 이의제기방법을 정보주체에게 알려야 함

3) 개인정보의 정정·삭제(제36조)

- 정보주체는 개인정보 정정·삭제 요구서를 해당 개인정보처리자에게 제출하여 그 개인정보의 정정 또는 삭제 요구 가능

  ※ 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우 그 삭제를 요구할 수 없고, 이를 해당 정보주체에게 알려야 함
- 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고 지체 없이 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 함

  ※ 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있음
- 요청일로부터 10일 이내에 조치 사실 또는 미조치 사실 및 이유·이의제기방법을 정보주체에게 알려야 함

4) 개인정보의 처리정지 등(제37조)

- 정보주체는 개인정보 처리정지 요구서를 개인정보처리자에게 제출하여 자신의 개인정보 처리 정지 요구 가능
- 처리 정지를 요구받은 때에는 지체 없이 개인정보 처리의 전부 또는 일부를 정지하고 해당 개인정보의 파기 등 필요한 조치를 하여야 함
- 다음 중 어느 하나에 해당하는 경우 처리정지요구를 거절할 수 있고, 그 사유를 지체 없이 해당 정보주체에게 알려야 함
  - 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
  - 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해 할 우려가 있는 경우
  - 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수없는 경우
  - 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우
- 요청일로부터 10일 이내에 조치 사실 또는 미조치 사실 및 이유·이의제기방법을 정보주체에게 알려야 함

나. 정보주체의 피해구제

1) 침해 사실의 신고 등(제62조)

- 개인정보에 관한 권리 또는 이익을 침해받은 사람은 개인정보보호위원회에 신고
- 개인정보침해 신고센터는 다음의 업무를 수행
  - 개인정보 처리와 관련한 신고의 접수·상담
  - 사실의 조사·확인 및 관계자의 의견 청취 등

2) 개인정보 분쟁조정위원회(제40조~제50조)

- 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁조정을 신청할 수 있음

  ※ 분쟁조정위원회 : 개인정보에 관한 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리하며, 위원장 1인을 포함한 20인 이내의 위원으로 구성
- 분쟁조정위원회는 분쟁조정 신청을 받은 날로부터 60일 이내에 심사하여 조정안을 작성·제시, 분쟁조정 당사자는 15일 이내에 조정안 수락 여부 회신

> **※ 조정안 포함 내용**
> ① 조사 대상 침해행위의 중지
> ② 원상회복, 손해배상, 그 밖에 필요한 구제조치
> ③ 같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치

▪ 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생하는 경우 개인정보 분쟁조정위원회에 일괄적인 집단분쟁조정을 의뢰 또는 신청 가능

3) 손해배상책임(제39조)

▪ 정보주체는 개인정보처리자가 개인정보 보호법을 위반한 행위로 손해를 입으면 개인정보 처리자에게 손해배상을 청구할 수 있음

※ 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없음

▪ 개인정보처리자가 개인정보 보호법에 따른 의무를 준수하고 상당한 주의와 감독을 게을리 하지 아니한 경우 개인정보의 분실·도난·유출·변조 또는 훼손으로 인한 손해배상책임을 감경 받을 수 있음