

# 개인정보보호론

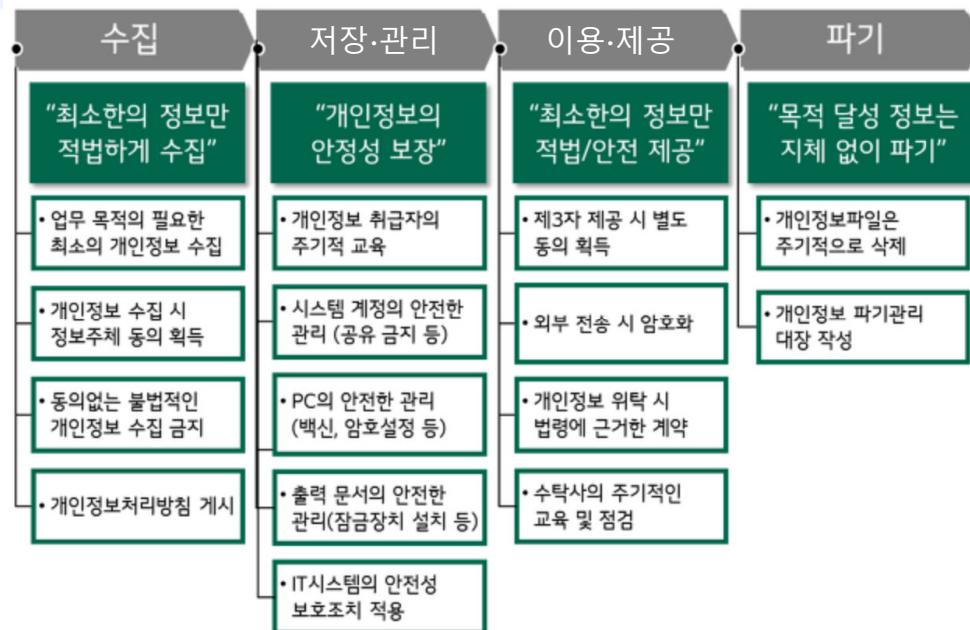
## [ 5주차. 개인정보 생명주기 ]

### 개인정보 생명주기(Lifecycle)

- 개인정보 생명주기 : 사람의 일생처럼 개인정보 관리 단계를 의미
  - 개인정보처리자가 개인정보를 “수집 – 저장/관리 – 이용 – 제3자 제공 – (보유기간이 종료된 이후) 파기”하는 일련의 단계



## 개인정보 처리자의 의무사항



## 수집단계 유출 흐름 분석

### ■ 개인정보 수집

- 개인정보를 수집할 때, 개인정보 처리자는 이용자에게 수집목적, 항목, 보유 및 이용기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 대한 불이익을 명시적으로 고지하고 동의를 얻어야 함
- 수집할 수 있는 최소한의 정보만을 수집해야 함
- 개인의 권리나 이익을 뚜렷하게 침해할 우려가 있는 민감한 정보인 인종, 민족, 사상, 출신지, 정치적 성향, 범죄 기록 등은 수집해서는 안됨
- 14세 이하 아동의 개인정보의 수집, 이용, 제공에 대한 동의를 받기 위해서는 사전에 반드시 법정대리인의 동의를 받아야 함
- 법정대리인의 동의를 위한 법정대리인의 성명, 연락처 등 최소한의 정보를 수집할 수 있음

■ 개인정보 수집 시 침해요소가 될 수 있는 사항

- 동의 없이 개인정보를 수집할 때, 고지사항을 이행하지 않는 경우
  - ✓ 인터넷 쇼핑몰 등에서 개인정보에 대한 수집목적, 이용목적, 보유기간, 회원탈퇴 방법 등에 대한 사항이 고지되지 않는 경우
- 동의 및 고지 없이 개인정보 주체 외로부터 개인정보를 수집하는 경우
  - ✓ 인터넷 마케팅 업체들이 쿠키를 사용해서 소비자들의 패턴과 거래내역을 동의를 구하지 않고 모니터링 하는 행위
- 법정대리인의 동의 없이 개인정보를 수집하는 경우
  - ✓ 법정대리인(부모)의 동의 없이 만 14세 어린이를 회원으로 가입시켜 게임, 아이템 등을 결제하게끔 하는 행위

■ 개인정보 수집 시 침해요소가 될 수 있는 사항

- 서비스 이용과 관련 없는 과도한 개인정보를 수집하는 경우
  - ✓ 인터넷 회원가입 시, 최소한의 개인정보를 넘어서 개인정보를 필수항목으로 입력하는 경우
- 해킹 등 불법 수단을 사용하여 개인정보를 수집하는 경우
  - ✓ 해킹 도구를 이용하여 키보드를 해킹하거나 웹 취약점을 이용하여 개인정보를 수집하는 경우
- 기만에 의해 개인정보를 수집하는 경우
  - ✓ 계약직 직원 등을 모집한다고 인터넷에 글을 올리고 회원 가입 시 많은 양의 개인정보를 입력하게 한 후, 이와는 상관없는 다른 사이트에 마케팅 등의 수단으로 수집한 해당 개인정보를 판매하거나 제공하는 경우

## 저장·관리단계 유출 흐름 분석

### ■ 개인정보 저장 및 관리

- 수집된 개인정보를 데이터베이스 등에 저장하고, 개인정보 보호정책에 따라 허가 받은 자만이 해당 개인정보에 접속할 수 있는 권한을 가지며 관리가 이루어짐
- 이용자가 서비스에 대한 탈퇴를 요청하면 해당 개인정보에 대한 이용 및 제공은 종료되어 서비스 탈퇴자의 개인정보는 즉시 파기되어야 함
  - ✓ 단, 법률적인 근거에 의해 개인정보를 일정기간 보유해야 하는 경우가 있으므로 서비스 탈퇴자의 개인정보는 종류에 따라 지체 없이 파기되거나 보유기간 동안 관리체계에서 파기 전까지 저장하고 관리
- 저장된 개인정보에 대한 다양한 보호조치를 취해야 할 뿐만 아니라, 개인정보의 이용시 발생할 수 있는 불법적인 개인정보 유출을 방지해야 함
  - ✓ 계정 및 비밀번호의 관리, 데이터베이스 접근 통제 정책, 개인정보 데이터베이스 쿼리의 무결성 검증, DB보안 관리자의 직무분리 등을 주기적으로 시행함으로써 안전한 저장 및 관리 요건을 충족시킬 수 있음

### ■ 개인정보 저장 및 관리 시 침해요소가 될 수 있는 사항

- 조직 내부 취급자에 의한 개인정보의 유출, 훼손, 변경
  - ✓ 개인정보의 노출은 이용자의 동의 없이 개인정보가 노출되거나 권한 관리 또는 시스템/서비스 오류를 통해 노출될 수 있음
- 외부인의 불법적 접근에 의한 개인정보 유출 및 훼손, 변경
  - ✓ 타인의 개인 메일 ID와 비밀번호를 알아내어 무단으로 메일 및 개인 웹사이트의 내용을 열람 등의 사례
- 사업자의 인식부족, 과실 등으로 인한 개인정보의 공개
  - ✓ 관리자가 실수로 이메일 첨부 파일에 개인정보를 포함한 파일을 전송하거나 홈페이지 상에 개인정보를 게재하는 경우

- 개인정보 저장 및 관리 시 침해요소가 될 수 있는 사항
  - 기술적, 관리적 조치 미비로 인한 개인정보의 유출
    - ✓ 사업자는 수집한 이용자의 개인정보가 외부 시스템 침입 등을 통해서 불법적으로 유출되는 사고에 대비해야 함
    - ✓ 개인정보의 저장은 저장하는 개인정보 항목별로 개인정보 보호정책에서 명시한 개인정보 보유기간에 따라 저장되어야 함
  - 고객의 개인정보 클레임에 대한 불응 또는 미조치
    - ✓ 이용자가 자신의 개인정보에 대한 삭제를 요구하거나 서비스 탈퇴를 요구했으나, 인터넷 서비스의 탈퇴 방법이 없거나 탈퇴신청 후에도 처리가 되지 않아 요금 부과 및 광고성 메일이 지속적으로 발송되는 경우

## 이용·제공단계 유출 흐름 분석

- 개인정보 이용 및 제공
  - 개인정보처리자가 이용자로부터 수집한 개인정보는 수집 및 이용 목적에 한하여 사용해야 하며 수집, 이용 목적이 변경되는 경우에는 반드시 이용자에게 별도의 동의를 구해야 함
  - 개인정보처리자는 아래의 경우를 제외하고는 개인정보를 수집할 때, 고지 및 이용자들이 동의한 범위를 넘어서 개인정보를 이용할 수 없음
    - ✓ 이용자의 동의를 얻은 경우
    - ✓ 요금 정산을 위해 필요한 경우
    - ✓ 사람의 생명 및 신체에 긴급한 위험이 발생한 경우로서 이용자의 동의를 받을 수 없는 정당한 사유가 있는 경우
    - ✓ 기타 법률에 특별한 규정이 있는 경우

## ■ 개인정보 이용 및 제공

- 이용자로부터 수집한 개인정보를 개인정보처리자에게 영리적으로 제공하는 경우는 '제3자 제공' '개인정보의 취급 위탁' 으로 구분할 수 있음
  - ✓ 제3자'에게 개인정보를 제공하는 경우: 제공받는 자, 제공받는 자의 개인정보 이용목적, 제공하는 개인정보 항목, 제공받는 자의 개인정보 보유 및 이용기간을 명시적으로 고지한 후, 동의를 획득해야 함
  - ✓ 취급 위탁의 경우: 개인정보 수집, 보관, 처리, 이용, 제공, 관리, 파기 등의 취급업무를 제3자에게 위탁할 때에는 개인정보 취급을 위탁 받는 자와 위탁 내용을 명시적으로 고지한 후, 동의를 구해야 함

## ■ 개인정보의 이용 및 제공 단계에서의 침해요인과 방법

- 동의 없는 개인정보의 무단 제공 및 공유
  - ✓ 개인정보 보호정책에 명시되지 않은 위탁사업자나 제3서비스 제공자에게 개인정보를 제공하는 경우
  - ✓ 개인정보 보호정책에 명시되지 않은 개인정보 항목을 제공하는 경우
  - ✓ 온라인 또는 오프라인 개인정보를 제3자에게 양도하는 등 불법적 거래의 경우
- 당초 수집 시 고지한 이용 목적을 넘어서는 개인정보의 이용
  - ✓ 사업자가 보유한 개인정보를 바탕으로 서비스 이용자에게 이메일, SMS, 휴대전화 등으로 사전 동의를 거치지 않고 상품광고나 광고성 정보를 제공하는 경우

## ■ 개인정보의 이용 및 제공 단계에서의 침해요인과 방법

### – 타인의 개인정보를 무단으로 이용하는 경우

- ✓ 개인정보는 서비스 필요성에 의해 분석이 필요한 경우도 있으나, 마케팅이나 기타 다른 목적으로 분석이 이루어지는 경우
- ✓ 사용자의 동의 없이 개인정보를 분석하는 경우로 수집 시점 또는 분석 이전에 개인정보의 분석에 대한 동의를 받지 않거나, 동의를 받았더라도 사전에 명시한 분석 목적 외로 사용, 또는 분석을 위한 개인정보 항목 외의 다른 개인정보를 분석에 포함시킨 경우가 모두 포함됨

## 파기단계 유출 흐름 분석

## ■ 개인정보의 파기

- 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적이 달성된 경우에는 개인정보를 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기해야 함
- ‘지체 없이’란 ‘즉시’를 의미하지 않으며, 합리적 근거 및 이유에 따라 가장 빠른 시기를 의미함
- 법령 등에 의하여 개인정보를 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보 파일을 다른 개인정보와 분리하여서 저장, 관리하여야 하며, 파기하는 경우는 다음과 같음
  - ✓ 개인정보의 수집, 이용 목적을 달성한 경우
  - ✓ 개인정보의 보유 및 이용 기간이 끝난 경우
  - ✓ 폐업하는 경우
  - ✓ 예외: 국세기본법, 전자상거래상에서의 소비자 보호에 관한 법률, 통신비밀 보호법

## ■ 개인정보의 파기

- 개인정보의 파기 대상은 이용자가 제공한 개인정보 뿐만 아니라 이용자로부터 서비스 제공 과정에서 생성된 개인정보인 로그인 기록, IP, 쿠키, 결제 기록 및 백업 파일에 기재된 개인정보도 포함됨
- 전자적으로 기록된 개인정보를 파기할 때에는 재생할 수 없는 기술적 방법으로 삭제하거나 당해 개인정보가 기록된 매체를 물리적으로 분쇄 또는 완전히 파기해야 함

## ■ 개인정보 파기 단계에서의 침해 요인과 방법

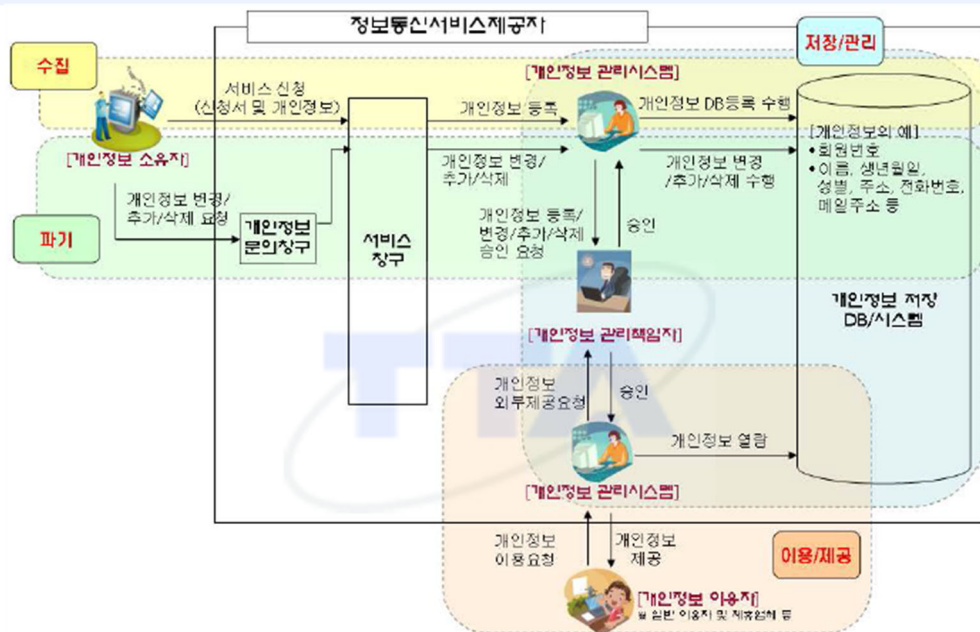
- 수집 및 목적 달성 후 개인정보를 파기하지 않는 경우
  - ✓ 개인정보를 파기하는 시점에서 파기가 성공적으로 수행되지 않는 경우에는 부적절한 개인정보의 파기가 발생함으로써 침해 위험이 존재
  - ✓ 일례로 개인정보가 저장된 하드디스크를 파기하는 경우, 저장 정보를 삭제하지 않고 그대로 방치하는 경우, 자석식 소거기나 소각기 등을 이용하지 않고 포맷하는 경우 등은 하드디스크 재생을 통해 개인정보가 유출될 수 있음
- 개인정보의 삭제 요구에 불응
  - ✓ 이용자가 자신의 개인정보를 삭제할 것을 요구했음에도 불구하고, 지체 없이 파기하지 않음으로써 해당 개인정보가 다른 목적으로 이용되거나, 노출될 수 있는 침해 위험이 존재할 수 있음



## 개인정보 생명주기 보안 관리모델

- 개인정보 생명주기별 보안 관리모델 (TTAS.KO-12.0053) 은 개인정보를 수집 및 저장, 관리, 이용하는 정보통신 서비스 제공자가 고객의 개인정보를 안전하고 효율적으로 관리할 수 있도록 제시된 표준

– \*한국정보통신기술협회(TTA) 표준화위원회



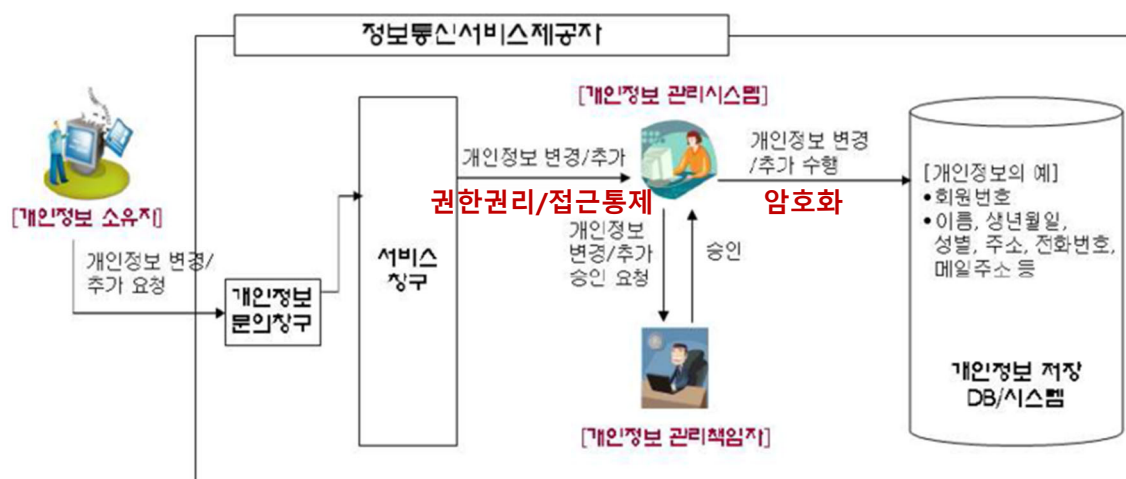
## 수집단계

- 서비스 제공자가 서비스를 이용하고자 하는 개인정보 소유자의 개인정보를 수집하는 단계
  - 개인정보처리자는 개인정보 소유자로부터 서비스 제공, 마케팅을 위해 개인 식별정보를 수집
  - 개인정보 소유자는 서비스 이용 신청(가입)과 동시에 자신의 개인정보를 서비스 제공자에게 제공하며, 개인정보 관리책임자의 승인하에 개인정보 데이터베이스에 등록



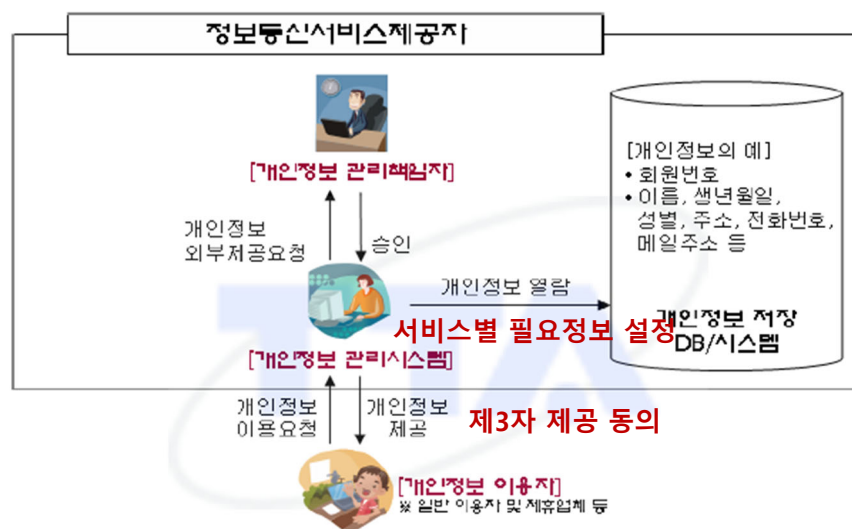
## 저장·관리 단계

- 정보통신서비스 제공자가 개인정보 소유자의 개인정보를 저장하고 이를 관리하는 단계
  - 소유자 등으로부터 수집한 개인정보는 데이터베이스에 저장되며, 여기 저장 단계에는 저장된 개인정보를 관리하는 내용도 포함
  - 관리란, 개인정보보호 정책에 따라 권한이 부여된 취급자 등만이 개인정보를 활용할 수 있도록 하는 것으로 권한관리, 암호화 등이 포함
  - 개인정보 소유자의 요청이 있는 경우, 책임자의 승인 하에 해당 개인정보를 변경·추가·파기



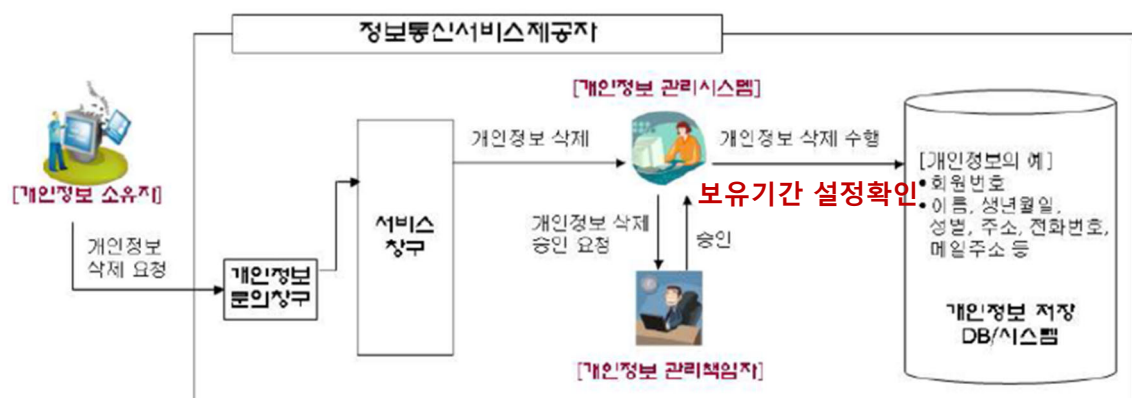
## 이용·제공 단계

- 정보통신서비스 제공자가 개인정보 소유자의 개인정보를 여러 가지 필요에 의해 이용하는 단계
  - 이용자가 수집 및 저장하여 보유하고 있는 개인정보를 회원인증, 서비스제공, 제품홍보, 요금정산, 제품배달, 민원처리 등에 사용
- 서비스 이용자 인증이나 인터넷 쇼핑 등의 기본 서비스 및 이벤트 등의 부가 서비스를 위해 이용
- 필요에 의해 개인정보보호정책에 명시하고 서비스 제공자 외 제3서비스 제공자(위탁업체, 제휴업체)에 제공



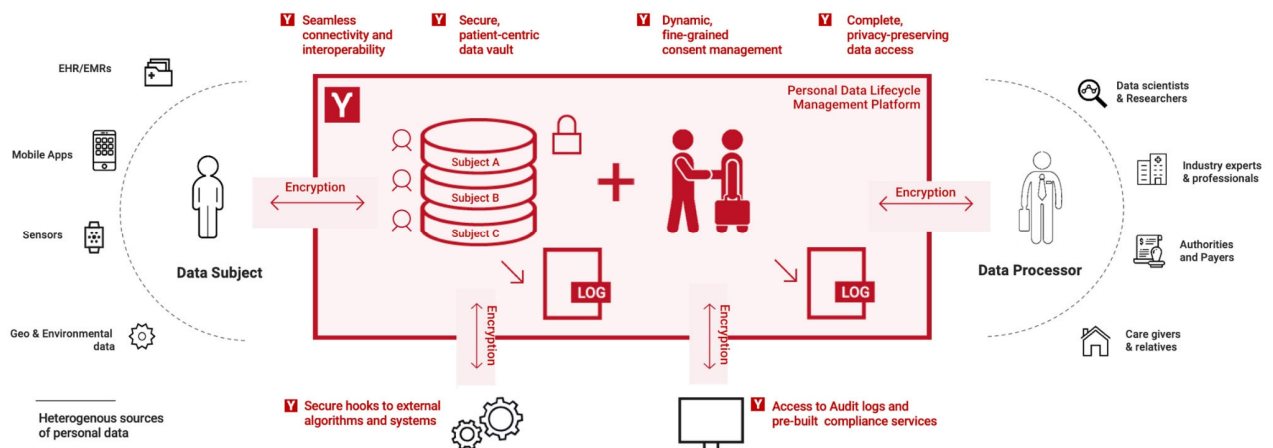
## 파기단계

- 정보통신서비스 제공자가 개인정보 소유자의 개인정보를 해당 정보의 보유기간이 종료하면 즉시 파기하는 단계
  - 서비스 제공자는 수집한 목적이 달성되면 개인정보를 지체없이 파기
  - 소유자가 회원 탈퇴를 하거나 IT 기업이 폐업하는 경우, 또는 특정 이벤트가 종료되는 등의 경우



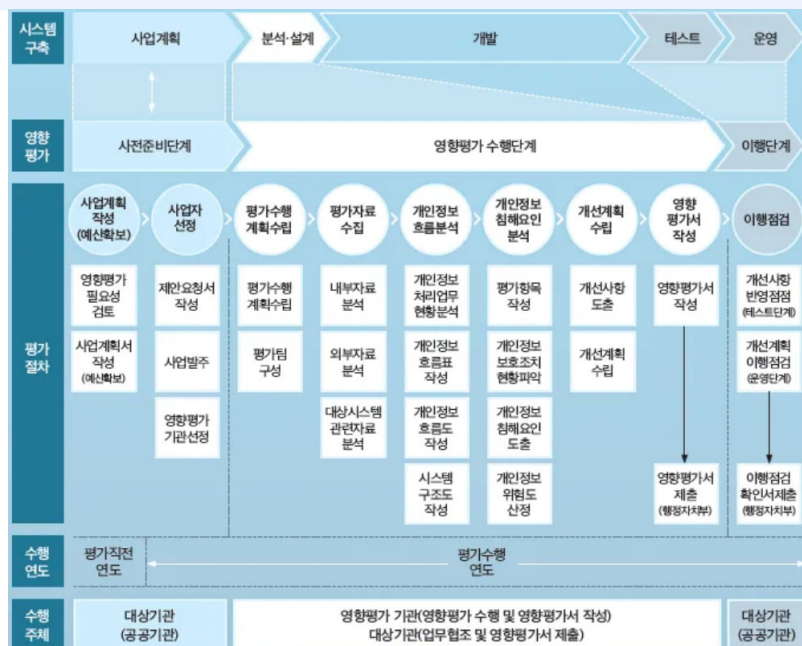
# 개인정보흐름 분석

- 어떤 데이터가 들어오는지
- 어떤 과정이 필요한지
- 어떤 조치를 취해야 하는지



## 개인정보 영향평가제도

- 새로운 정보시스템의 도입과 개인정보의 수집에 앞서 계획하고 있는 시스템이 구축, 운영될 경우 프라이버시에 미칠 영향에 대하여 미리 조사, 예측, 검토하는 체계적인 절차를 의미
- 개인정보 영향평가 범위
  - 개인정보를 다량으로 보유, 관리하는 정보시스템의 신규 구축
  - 신기술 또는 기존 기술의 통합으로 프라이버시 침해 가능성이 있는 기술을 사용하는 사업
  - 개인정보를 보유, 관리하는 기존 정보 시스템을 변경하는 경우
  - 개인정보 생명주기 단계에서 침해 우려가 발생할 수 있는 사업
  - 기존에 보유하고 있는 개인정보 파일을 다른 기관과 연계하는 경우



■ 1. 영향평가계획 수립  
- 평가과정에 필요한 사항들을 정리

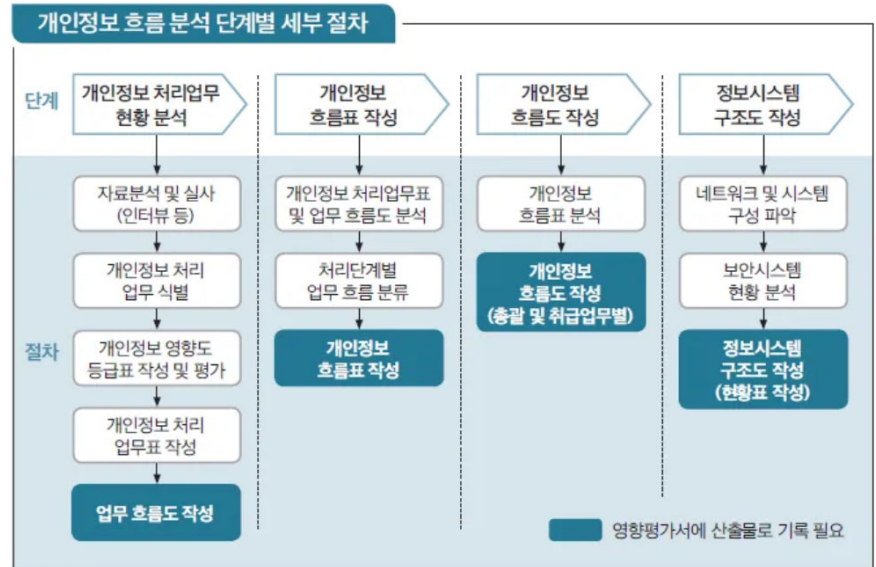
목차	주요 내용	참고자료
1. 평가 목적	영향평가 수행 필요성 및 추진 배경 등을 기술	필요성 검토 질문서
2. 평가 대상	평가대상이 되는 정보화사업(정보시스템)명칭 기술	제안요청서(RFP), 사업계획서 등
3. 평가 주체	영향평가팀 구성 현황	영향평가팀 구성 및 운영 계획서
4. 평가 기간	영향평가 착수시점부터 완료시점까지의 평가기간을 산정하여 기술	영향평가기관 선정 단계에서 산출물 및 협의내용, 영향평가 수행안내서 참고
5. 평가 절차(방법)	영향평가 수행안내서 등을 참조하여 평가 절차 및 단계별 주요 수행사항 및 기간 등 기술	
6. 주요 평가사항	중점적으로 평가되어야 하는 사항 기술	
7. 평가기준 및 평가항목	영향평가 수행안내서에서 표준적으로 요구되는 평가항목 (표)와 해당 사업의 특정 IT 기술 활용 여부 확인 ※ 부록으로 영향평가 항목 첨부	
8. 자료수집 및 분석계획	영향평가 수행 시 분석하여야 하는 관련 참고자료를 확인하여 해당 기관과 관련 있는 자료 파악	개인정보 관련 정책, 법규 검토 단계의 산출물 참조
9. 평가결과 정리	영향평가 결과로 도출된 산출물(보고서)과 이를 활용하여 당해 사업에 적용하기 위한 방안 등 기술	영향평가팀 회의 내용 등 참조

■ 2. 평가자료 수집

항목	수집 목적	수집 대상 자료
① 내부 정책 자료	▶ 기관 내부의 개인정보보호 체계, 규정, 조직 현황 등 분석	• 기관 내 개인정보 보호 규정 • 기관 내 정보보안 관련 규정 • 기관 내 직제표 등
	▶ 개인정보취급자(정보시스템 관리자, 접근자 등), 위탁업체 등에 대한 내부 규정 및 관리·교육 체계 확인	• 개인정보 관련 조직 내 업무 분장표 및 직급별 권한 • 정보시스템의 접근권한에 대한 내부 규정 • 위탁업체 관리 규정 등 • 시스템 관리자 및 정보취급자에 대한 교육계획
② 외부 정책 자료	▶ 개인정보보호 정책 환경 분석	• 개인정보 보호법, 관련 지침 등 • 개인정보보호 기본계획 등
	▶ 영향평가 대상사업의 특수성을 반영한 정책 환경 분석	• 평가대상사업 추진 근거 법률 및 개인정보보호 관련 법령
③ 대상시스템 관련자료	▶ 정보시스템을 통해 수집되는 개인정보의 양과 범위가 해당 사업 수행을 위해 적절하지 파악	• 사업 수행 계획서, 요건정의서 • 제안서, 업무기능분해도 • 업무흐름도, 화면설계서
	▶ 정보시스템의 외부연계 여부 검토	• 위탁 계획서, 연계 계획서 • 인터페이스 정의서 • 메뉴 구조도
	▶ 정보시스템의 구조와 연계된 개인정보 보호 기술 현황 파악	• 침입차단시스템 등 보안 시스템 구조도 등 • 인터페이스 정의서



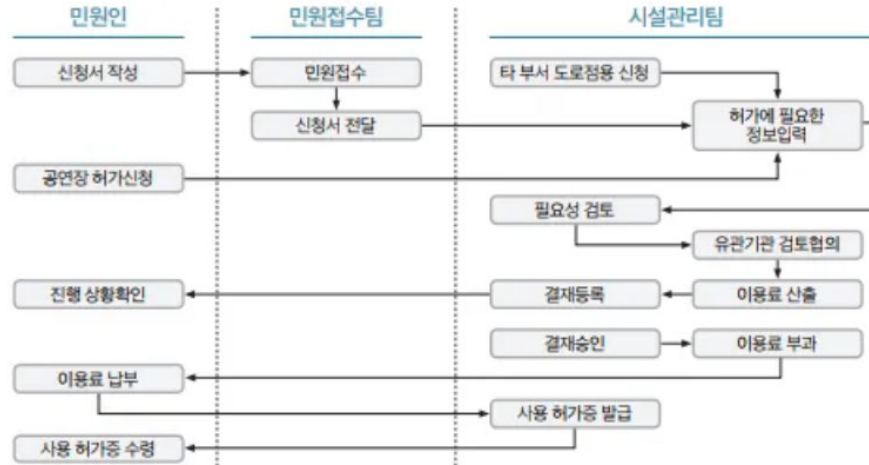
### 3. 개인정보 흐름분석



#### 3-1. 개인정보 처리업무 현황 분석 – 개인정보처리 업무표 작성

평가 업무명	처리 목적	처리 개인정보	주관 부서	개인정보 건수 (고유식별정보수)	개인정보 영향도
회원 관리	홈페이지 회원가입, 본인확인, 정보제공 등 회원 서비스 제공	필수 : 성명, 생년월일, 전화번호, 이메일주소, ID, 비밀번호 선택 : 집주소, 집전화번호	민원팀	10만건 (0건)	5
상담 업무	고객 문의 및 민원 응대	필수 : 성명, 전화번호, 상담내용	민원팀	5천건 (0건)	3
실업급여 관리	실업급여 지급확인 및 관련 절차 알림, 확인	필수 : 성명, 주민등록번호, 계좌번호, 전화번호 선택 : 이메일주소	민원팀	3만건 (3만건)	5
...	...	...	...	...	...

## – 개인정보 업무 흐름도 작성



### 3-2. 개인정보 흐름표 작성

수집 흐름표

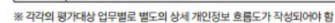
평가 업무명	수집					
	수집 항목	수집 경로	수집 대상	수집 주기	수집담당자	수집 근거
민원 처리	성명, 주민등록 번호, 전화번호, 이메일 주소, 민원 내용	온라인 (홈페이지)	민원인	상시	-	이용자 동의/ ○○법제○조○항 (주민등록번호)
		오프라인 (민원신청서 작성)	민원인	상시	안내창구 담당자	이용자 동의/ ○○법제○조○항 (주민등록번호)

보유·이용 흐름표

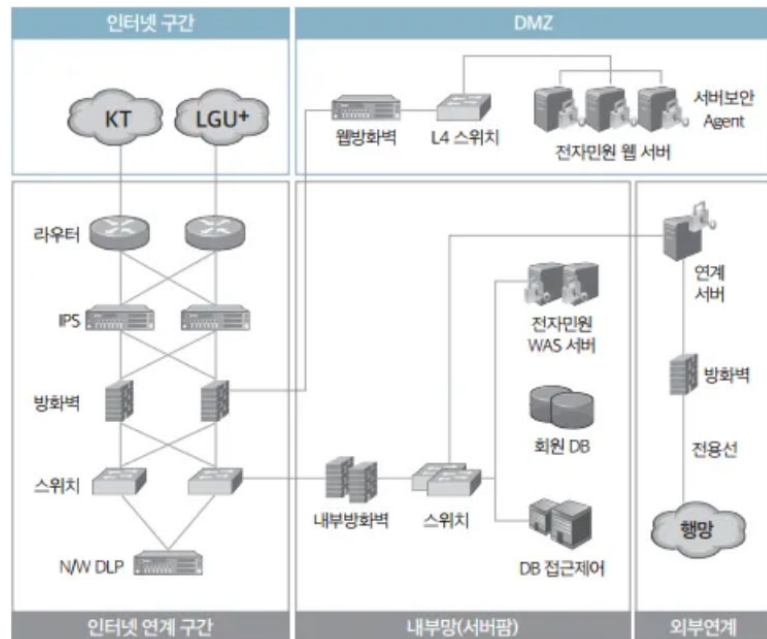
평가 업무명	보유·이용							
	보유형태	암호화 항목	민원 처리			통계 관리		
			이용 목적	개인정보 취급자	이용 방법	이용 목적	개인정보 취급자	이용 방법
민원 처리	Web DB	주민등록번호, 비밀번호(일방향)	민원 처리 및 결과 관리	민원처리 담당자, 민원 관련 업무 담당자	A기관 홈페이지	민원 현황 조회	통계 담당자	관리자 홈페이지
	민원 DB	주민등록번호, 비밀번호(일방향)						
	캐비넷 (신청서류철)	-						

평가 업무명	제공							파기				
	제공 목적	제공자	수신자	제공 정보	제공 방법	제공 주기	암호화 여부	제공 근거	보관 기간	파기 담당자	파기 절차	분리 보관 여부
민원 처리	민원 처리 실적 집계	통계 담당자	OO 도청	민원인 성명, 민원 접수 내용, 처리 결과	실시간 DB 연동	상시	통신구간 암호화 (VPN)	전자 정부법 시행령 OO조	민원 처리 완료 후 1년	DB 관리자	일단위 DB 파기	별도 보존 DB 구성
									민원 DB 입력 후 스캔 후 파기	통계 담당자	주단위 문서 절단	-

- 1) 총괄흐름도 작성
- 2) 업무별 흐름도 작성



### 3-4 정보시스템 구조도 작성



39

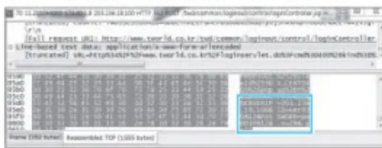
## 4. 개인정보 침해요인 분석

### 4-1. 평가항목 구성

- ✓ 5개 영역 25개 세부 평가분야
  - ① 대상 기관의 개인정보보호 관리체계
  - ② 대상 시스템의 개인정보보호 관리체계
  - ③ 개인정보 처리단계별 보호조치
  - ④ 대상 시스템의 기술적 보호조치
  - ⑤ 특정 IT기술 활용 시 개인정보보호

40

## 4-2 개인정보 보호조치 현황파악(항목별 평가)

질문의 코드	질문	확인			
		이행	부분이행	미이행	해당없음
4.3.2	<ul style="list-style-type: none"> <li>고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하도록 계획하고 있습니까?</li> </ul>			○	
평가 근거 및 의견	<ul style="list-style-type: none"> <li>○○○ 웹사이트에 보안서버(SSL)가 적용되어 있지 않아 인터넷 회원의 인증정보(ID/PW), 고유식별정보 등 개인정보가 인터넷 구간에서 평문으로 전송되고 있음</li> </ul> <p>[회원 로그인시 전송 데이터 캡처 결과 - ID/PW 평문 노출]</p> 				
항목 설명	<ul style="list-style-type: none"> <li>웹사이트에서 ID/PW와 같은 인증정보, 고유식별정보 등 중요 개인정보를 전송하는 경우, 네트워크 도청을 통한 개인정보 노출을 방지하기 위하여 인증정보를 포함한 개인정보에 대하여 암호화하여 전송하도록 함</li> </ul>				
평가 예시	<ul style="list-style-type: none"> <li>이행 : 웹사이트에 보안서버(SSL)를 적용하여 인증정보, 고유식별정보 등 개인정보를 암호화하여 전송함</li> <li>부분 이행 : 웹사이트에 보안서버(SSL)를 적용하여 개인정보를 암호화하여 전송하고 있으나, 비밀번호 변경 등 일부 화면에서 암호화 전송이 누락됨</li> </ul>				
관련 법률 및 문서	<ul style="list-style-type: none"> <li>개인정보의 안전성 확보조치 기준 고시 제6조(개인정보의 암호화)</li> </ul>				

41

## 4-3 개인정보 침해요인 도출

질문의 코드	질문	평가근거 및 의견	개인정보 침해 요인	법적 준거성
4.3.2	<ul style="list-style-type: none"> <li>고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하도록 계획하고 있습니까?</li> </ul>	<ul style="list-style-type: none"> <li>현 시스템 및 설계서 상에 고유식별정보 등 개인정보를 홈페이지 서버로 전송 시 암호화가 적용되어 있지 않음</li> </ul>	<ul style="list-style-type: none"> <li>스니핑 등 네트워크 도청을 통해 홈페이지 회원의 고유식별정보, 인증정보가 비인가자에게 누출될 우려가 있음</li> </ul>	<ul style="list-style-type: none"> <li>개인정보 안전성 확보조치 기준 고시 제6조 위반</li> </ul>

42

- 4-4 개인정보 위험도 산정
  - 위험도 = 개인정보 영향도 + (침해요인 발생가능성 x 법적 준거성) x 2

개인정보 영향도(자산 가치)

등급	설명	자산가치
1등급	- 그 자체로 개인 식별이 가능하거나 민감한 개인정보 - 관련 법령에 따라 처리가 엄격히 제한된 개인정보 - 유출 시 범죄에 직접적으로 이용 가능한 정보	5
2등급	- 조합되면 명확히 개인의 식별이 가능한 개인정보 - 유출 시 법적 책임 부담 가능한 정보	3
3등급	- 개인정보와 결합하여 부가적인 정보 제공 가능 정보 - 제한적인 분야에서 불법적 이용 가능 정보	1

법적 준거성 가중치 부여

구분	법적 준거성	중요도
높음	법적 준수 사항	1.5
낮음	법률 외 요건	1

개인정보 침해요인 발생가능성

구분	발생 가능 정도	중요도
높음	즉각적인 침해 발생 가능성이 있는 경우	3
중간	침해발생 가능성이 존재하지만 즉각적이지는 않는 경우	2
낮음	침해발생 가능성이 희박한 경우	1

위험도 범위

구분	산정식	위험도
최대값	위험도 = 5 + (3 × 1.5) × 2	14
최소값	위험도 = 1 + (1 × 1) × 2	3

개인정보 처리 업무명	처리 개인정보	개인 정보 영향도	질문의 코드	침해요인	발생 가능성	법적 준거성	위험도
회원가입 (수집)	성명, 주민등록번호, 전화번호, 이메일주소, 퇴직정보	5	2.2.1	변경된 부분에 대한 정보가 반영되지 않아 개인정보파일 현황을 적절히 파악하지 못해 보유하고 있는 개인정보의 관리가 어려움	3	1.5	14
회원가입 (보유-이용)	성명, 주민등록번호, 전화번호, 이메일주소, 퇴직정보	5	3.4.1	정보주체가 위탁되는 개인정보 항목 및 위탁 목적 등을 알 수 없게 되어 정보주체의 권리를 제한할 수 있음	3	1.0	11
회원가입 (보유-이용)	성명, 주민등록번호, 전화번호, 이메일주소, 퇴직정보	5	4.3.1	개인정보유출 사고가 발생 시 개인정보를 취득한자가 개인정보를 손쉽게 이용할 수 있음	2	1.0	9
회원가입 (파기)	성명, 주민등록번호, 전화번호, 이메일주소, 퇴직정보	5	3.5.1	관련 법률을 위반하여 징계나 형사 벌금 등의 처벌을 받을 수 있음	3	1.5	14



- 5. 개선계획 수립
  - 5-1 개선방안 도출
  - 5-2 개선계획 수립

우선순위	개선과제명	개선내용	담당부서	수행시기
1	개인정보보호 교육 강화	• 개인정보보호 교육계획 수립(2.1.2) • 개인정보취급자에 대한 교육 수행 (2.1.2)	고객보호팀	사업종료전 (2016.06)
2	개인정보 수집시 보안강화	• 회원 가입 시 입력받는 개인정보 수집항목 최소화(3.1.2) • 회원정보 DB 저장시 암호화 등의 설계 변경(4.3.1)	사업주관 부서	사업종료전 (2016.06)
3	개인정보취급자 PC 보안강화	• 개인정보취급자 단말기에 키보드 해킹방지 솔루션 도입(4.8.2) • PC에 개인정보파일 저장시 암호 설정(4.3.1)	사업주관 부서	2차 사업 (2017 상반기)
...	...	...	...	...

- 6. 영향평가서 작성

목차	주요 내용
표지	▶ 대상 사업명, 날짜, 사업 수행 부서 등 기재
요약	▶ 영향평가에 대한 간략한 요약, 획득한 결론과 개선 사항들을 요약된 형태로 기술
목차	▶ 영향평가서의 주요 장과 절, 그리고 이들이 수록된 페이지 번호를 명시
I. 추진 개요	
1. 사업(시스템)명	▶ 대상사업(시스템)명 기재
2. 추진 경과	▶ 평가팀 구성 등 영향평가 시작~종료시점까지 주요 경과 기술
II. 개인정보 흐름분석	
1. 필요성 검토 결과	▶ 필요성 검토 결과 기재
2. 개인정보 업무처리 흐름표	▶ 전체 업무 중 개인정보와 관련한 업무흐름
3. 개인정보 흐름표	▶ 개인정보 흐름표 제시 및 설명
4. 개인정보 흐름도	▶ 개인정보 흐름도 제시 및 설명
5. 시스템 구조도	▶ 대상사업의 시스템 구조도 제시
III. 영향평가 결과	
1. 대상기관 개인정보보호 관리체계	▶ 각 분야별 조치 현황 및 침해 요인 기술
2. 대상시스템의 개인정보보호 관리체계	
3. 개인정보 처리단계별 보호조치	
4. 대상시스템의 기술적 보호조치	
5. 특정 IT기술 활용시 개인정보 보호조치	
IV. 위험평가	
1. 위험평가 개요	▶ 위험평가 개요 기술
2. 위험평가 결과	▶ 위험평가 결과 기술
3. 개선방안 도출	▶ 도출된 개선사항 정리
4. 개선계획 수립	▶ 도출된 개선사항의 이행계획 수립
V. 총평	

## ❖ 개인정보 위험도 분석 재정리

