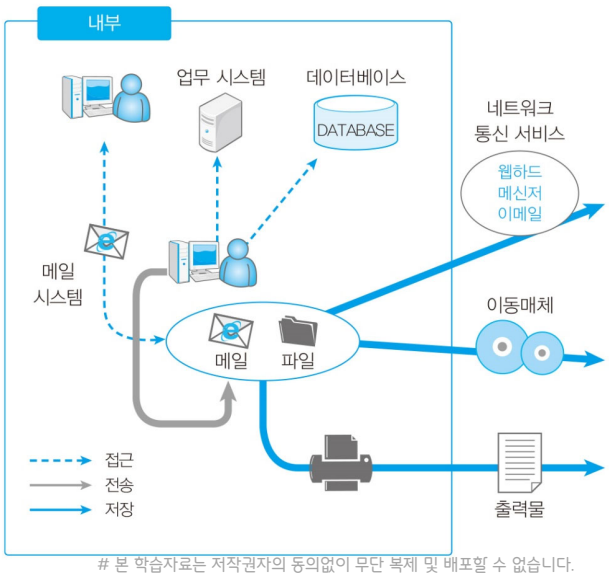
개인정보보호론

[안정성확보조치와 중간정리]

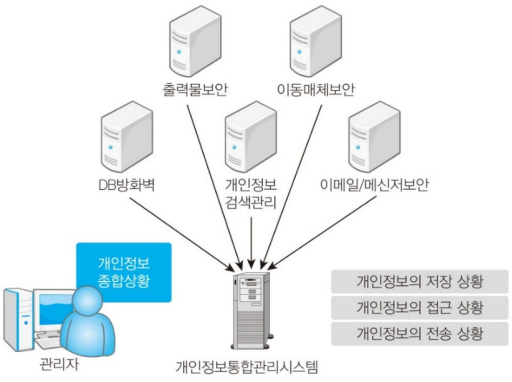
안전성확보조치

한 눈에 보는 정보 유출 단계



개인정보 생명주기 전체에 걸친 개인정보 종합 관리기술

- **개인정보 보호 관련 기술들은 각기 자신만의 보호 기술과 영역을 갖고 있음**
  - 해당 조항들을 만족시키기 위해서는 개인정보를 누가 보유하고 있고, 누가 접근했으며, 누가 외부로 전송하였는지 종합적으로 파악할 수 있어야 하며, 유출사고 발생 시 추적할 수 있는 인프라를 구축해야 함
  - 개인정보 종합관리 기술은 이 필요성을 만족시킬 수 있음



단계별 보안대책과 보호기술

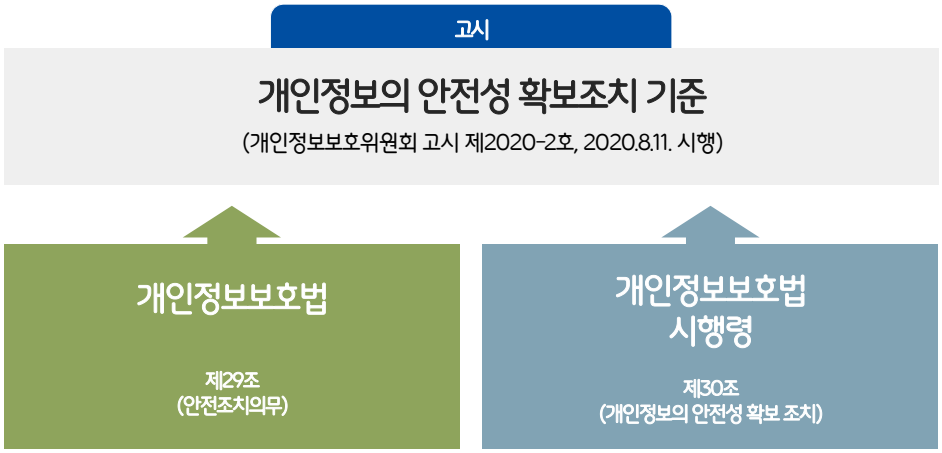
- **효과적으로 정보 유출을 방지하기 위해서는 접근, 저장, 전송 단계별로 보안대책이 필요함**

유출 단계	보안 대책	관련 보호기술/제품
접근	• 중요 정보의 접근 내역을 기록하고 감사 • 권한이 있는 사람만 정보에 접근할 수 있도록 통제 • 해킹을 통한 정보 획득을 차단	• DB보안 기술(DB암호화, DB방화벽) • 네트워크 DLP(이메일/메신저 보안 기술) • IPS/IDS • 방화벽/웹 방화벽 .PC보안/서버보안 기술 • 홈페이지 유출방지 기술
저장	• PC와 서버상에 저장되어 있는 중요 정보를 식별하고 (조직 상황에 따라) 중앙집중적 관리 • 업무상 필요한 정보는 암호화하여 보관 • 업무상 필요 없거나, 필요기간이 지나면 삭제	• 엔드포인트 DLP(개인정보 검색/관리 기술) • 문서 암호화 기술 • 파일 완전삭제 기술
전송	• 외부로 전송되는 정보 내역을 기록하고 감사 • 정당하지 않은 중요 정보의 외부전송 차단	• 이메일/메신저 보안 기술 • 엔드포인트 DLP(이동매체 보안 기술) • 출력물 보안 기술 • 보안서버 • VPN 기능

개인정보 생명주기별 기술적 보안 제품

수집	저장	이용	전송	폐기
키보드 보안	PC DRM	PC 보안 / 출력 보안	SSL	데이터완전삭제
온라인 PC 보안	서버 DRM	DB 접근제어 / 서버 보안	보안 메일	디가우저
SSL	DB 암호화	Data Masking	DRM	DRM
공인인증	보안 USB	웹 보안 / 개인정보필터링	외부전송 모니터링	문서파쇄기
I-PIN / G-PIN	로그 백업	EAM / IAM (계정/권한관리)	암호화 Toolkit	현장파쇄서비스
Paperless	테스트 데이터 변환	개인정보 감사 (Forensic)	보안 USB	해지 DB
개인영향평가시스템				
개인정보 오남용 / 정보유출 통합 모니터링(로그분석) 시스템				

법적 근거



목적과 용어의 정의

▪ [제1조] 안정성 확보조치 기준의 목적

개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보에 필요한
기술적 · 관리적 · 물리적 안전조치에 관한 최소한의 기준을 정하는 것

▪ [제2조] 사용하는 용어

- 정보주체
- 개인정보파일
- 개인정보처리자
- 대기업
- 중견기업
- 중소기업
- 소상공인

- 개인정보보호책임자
- 개인정보취급자
- 개인정보처리시스템
- 위험도분석
- 비밀번호

- 정보통신망
- 공개된 무선망
- 모바일 기기
- 바이오정보
- 보조저장매체
- 내부망
- 접속기록
- 관리용 단말기

※용어의 정의는 고시 참조

유형별 안전조치 적용

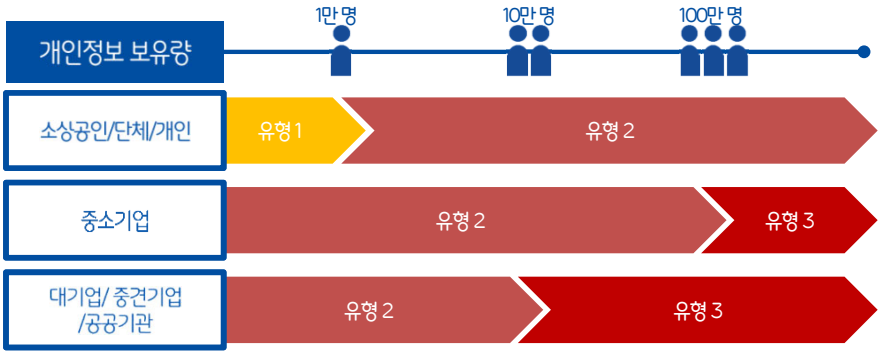
▪ [제3조] 안전조치 기준 차등 적용

[별표] 개인정보처리자 유형에 따른 안전조치 기준 차등 적용

유형1 (완화)	1만 명 미만의 개인정보를 보유한 소상공인, 단체, 개인
유형2 (표준)	1만 명 이상의 개인정보를 보유한 소상공인, 단체, 개인 10만 명 미만의 개인정보를 보유한 대기업, 중견기업, 공공기관 100만 명 미만의 개인정보를 보유한 중소기업
유형3 (강화)	10만 명 이상의 개인정보를 보유한 대기업, 중견기업, 공공기관 100만 명 이상의 개인정보를 보유한 중소기업

유형별 안전조치 적용

[제1조] 안정성 확보조치 기준의 목적



유형1 (완화)	유형2 (표준)	유형3 (강화)
• 제5조: 제2항~제5항 • 제6조: 제1항, 제3항, 제6항, 제7항 • 제7조: 제1항~제5항, 제7항 • 제8조, 제9조, 제10조, 제11조, 제13조	• 제4조: 제1항 제1호~제10호, 제15호, 제3항, 제4항 • 제5조 • 제6조:제1항부터 제7항까지 • 제7조:제1항부터 제5항까지, 제7항 • 제8조, 제9조, 제10조, 제11조, 제13조	• 제4조부터 제13조까지

내부 관리계획의 수립과 시행(제4조)

개인정보보호
내부 관리계획

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육

관리적

4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지

기술적

9. 물리적 안전조치
10. 개인정보 보호조직 구성·운영
11. 유출사고 대응계획 수립 · 시행
12. 위험도 분석 및 대응방안 마련
13. 재해 · 재난 대비 개인정보처리시스템의 물리적 안전조치
14. 개인정보처리 수탁자의 관리·감독

유형1 선택조항

15. 그 밖에 개인정보 보호를 위해 필요한 사항

물리적

Personal Information Protection Theory

내부 관리계획의 수립과 시행(제4조)

개인정보보호
내부 관리계획

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육

관리적

4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지

기술적

9. 물리적 안전조치
10. 개인정보 보호조직 구성·운영
11. 유출사고 대응계획 수립 · 시행
12. 위험도 분석 및 대응방안 마련
13. 재해 · 재난 대비 개인정보처리시스템의 물리적 안전조치
14. 개인정보처리 수탁자의 관리·감독

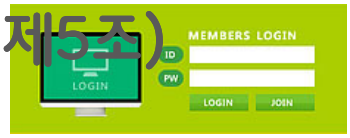
유형1 선택조항

15. 그 밖에 개인정보 보호를 위해 필요한 사항

물리적

상명대학교 SANGMYUNG UNIVERSITY
본 학습자료는 저작권자의 동의없이 무단 복제 및 배포할 수 없습니다.

접근권한의 관리(제5조)



① 개인정보처리시스템에 대한 접근 권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여

유형1 선택조항

② 전보, 퇴직 등의 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 접근 권한을 변경 또는 말소

③ 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 3년간 보관

④ 개인정보처리시스템의 사용자계정 발급시 개인정보취급자 별로 발급하며, 다른 개인정보취급자와 공유되지 않도록 함

⑤ 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용

⑥ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근 제한 등 필요한 기술적 조치

유형1 선택조항

접근통제(제6조)

① 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 기본 조치

1. 접속 권한을 IP주소 등으로 제한 → 인가 받지 않은 접근 제한
2. 접속한 IP주소 등을 분석 → 불법적인 개인정보 유출 시도 탐지 및 대응

→ 위 기능을 포함하여 조치해야 함

IP(Internet Protocol)

② 외부에서 개인정보처리시스템에 접속하려는 경우 안전한 접속수단 또는 안전한 인증수단 적용

유형1 선택조항

※ 가상사설망 (VPN : Virtual Private Network) 또는 전용선 등

③ 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 개인정보가 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등 조치 수행

접근통제 (제6조)

④ 인터넷 홈페이지를 통해 고유식별정보가 유출. 변조. 훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치 수행 ☑ 유형1 선택조항

⑤ 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 해야 함 ☑ 유형1 선택조항

⑥ 별도의 개인정보처리시스템이 아닌 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우

- 제1항 적용 안 함
- 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능 이용 가능

⑦ 업무용 모바일 기기의 분실. 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치

개인정보의 암호화(제7조)

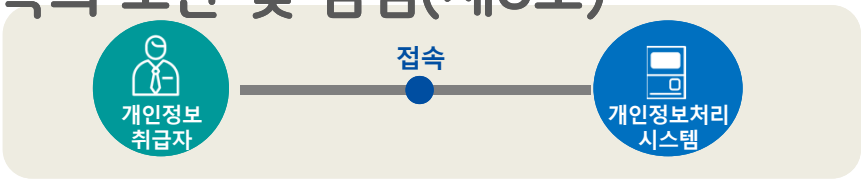
암호화 필요 대상: 고유식별정보, 비밀번호, 바이오정보

암호화 기준

구 분				암호화 기준
정보통신망, 보조저장매체를 통한 송, 수신 시	비밀번호, 바이오정보, 고유식별정보			암호화 송, 수신 ※제7조 ①항 TIP 참조
정보처리 시스템에 저장 시	비밀번호			일방향(해쉬 함수) 암호화 저장
	바이오정보			암호화 저장
	고유식별정보	주민등록번호		암호화 저장
		여권번호, 외국인등록번호, 운전면허번호	인터넷 구간, 인터넷 구간과 내부망의 중간 지점 (DMZ)	암호화 저장
			내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부. 적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장 시	비밀번호, 바이오정보, 고유식별정보			암호화 저장(비밀번호는 일방향 암호화 저장)

- 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행 ☑ 유형1,2 선택조항
- 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장

접속기록의 보관 및 점검(제8조)



① 접속한 기록을 **6개월 이상 보관. 관리**

② **반기별로 1회 이상** 점검 → 개인정보의 **분실. 도난. 유출. 위조. 변조 또는 훼손** 등에 대응하기 위하여

③ 개인정보취급자의 접속기록이 위. 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관

접속ID, 날짜와 시간, IP주소, 수행업무

정기적으로 백업 수행

정기 점검 / 후속 조치

악성프로그램 등 방지(제9조)

악성프로그램 등을 방지. 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치. 운영해야 함

1. 보안 프로그램은 항상 최신의 상태로 유지

- 자동 업데이트 기능 사용
- 일 1회 이상 업데이트 실시

2. 악성프로그램 관련 경보 발령 또는 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트 실시

3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

관리용 단말기의 안전조치(제10조)

개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로
개인정보처리시스템에 직접 접속하는 단말기

1 인가 받지 않은 사람이 임의로 조작하지 못하도록 조치

2 본래 목적 외로 사용되지 않도록 조치

3 악성프로그램 감염 방지 등을 위한 보안조치 적용

물리적 안전조치(제11조)

① 개인정보 보관을 위한 물리적 보관 장소(전산실, 자료보관실 등)는
출입통제 절차를 수립. 운영

② 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는
안전한 장소에 보관

③ 개인정보가 포함된 보조저장매체의 반출. 입 통제를 위한 보안대책을 마련

다만, 별도의 개인정보처리시스템 없이 업무용 컴퓨터 또는 모바일 기기를 이용하여
개인정보를 처리하는 경우는 예외

유형1,2 선택조항

재해·재난 대비 안전조치(제12조)

화재, 홍수, 단전 등의 재해. 재난 발생 시

① 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검

② 개인정보처리시스템 백업 및 복구를 위한 계획 마련

개인정보의 파기(제13조)

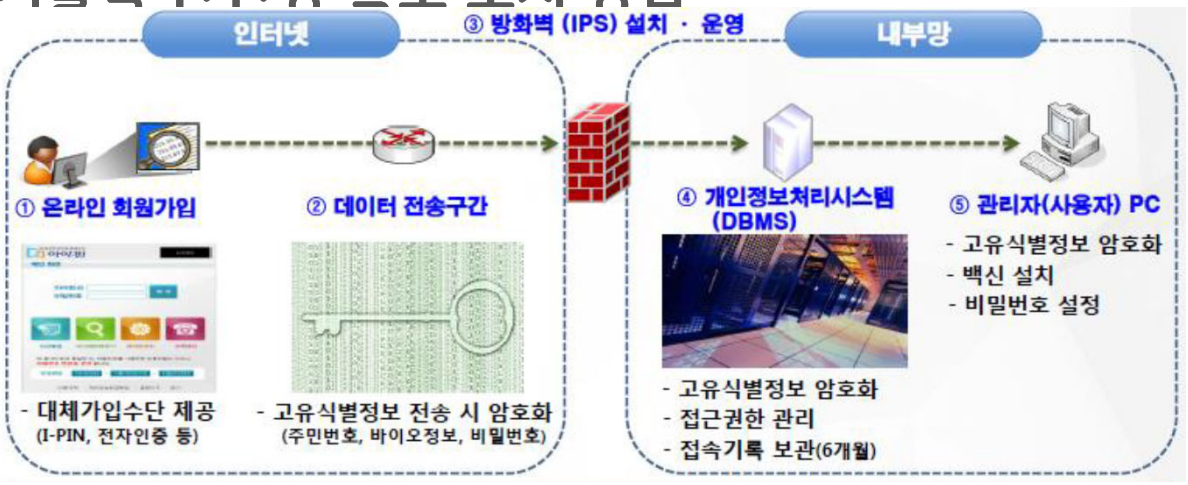
① 개인정보 파기 조치

1. 완전파괴(소각. 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 1항의 방법이 어려울 경우 일부 파기 조치

전자적 파일	개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
기록물, 인쇄물, 서면, 그 밖의 기록매체	해당 부분을 마스킹, 천공 등으로 삭제

기술적 안전성 확보 조치 종합



중간정리

개인정보보호론
[1주차. 개인정보개념]

정보에서의 “의미 "

- 정보란 어떤 데이터(자료)를 의도나 목적에 맞게 분석 혹은 가공하여 그 의미를 표현한 것

- 나에게 의미 있는 것은 정보, 나에게 의미 없는 것은 데이터
- 의미란 주관적으로 부여되는 것으로 개인 사고(思考)와 연결
  - 예. 아침 등교길 기억되는 사람

➢ 우리의 머릿속에 남아 있는 것은 모두 어떤 의미를 지니고 있는 ‘정보’

➢ 그래서 정보는 “생각의 표현 "

매체

- 매체 (= 미디어(Media))는 인간 상호간에 정보, 지식, 감정, 의사 등을 전달하는 모든 수단을 의미
- 인간은 매체를 통해 정보와 지식을 공유

- 마샬 맥루한(Marshall McLuhan) “매체는 메시지이다.”
  - 매체 자체가 메시지라고 선언
  - 테크놀로지와 직결되는 매체 자체가 그 내용인 메시지보다 더 중요하다.
  - 그의 매체 개념은 단순한 매스미디어 뿐만 아니라 인간이 고안한 도구나 기술을 포함한다.
  - 인간의 신체 및 감각기관의 기능을 확장하는 것은 모두 매체라고 본다.

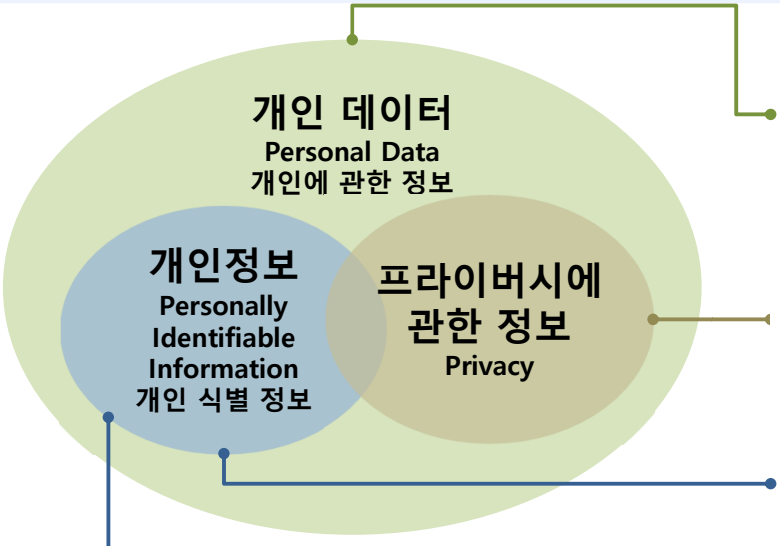
▶ 기술결정론적 관점

개인정보의 5가지 개념

- 1. 개인정보는 ‘살아 있는’ 개인에 관한 정보
- 개인정보는 ‘개인에 관한’ 정보
  - 사적 정보, 공적 정보, 공개된 정보 등 모두 포함
  - 정보의 내용이 개인에 관한 사항을 다루고 있는 경우
  - 정보의 목적 또는 정보처리의 목적이 개인에 관한 사항인 경우
  - 정보처리의 결과가 개인에 관한 사항인 경우
- 3. 개인정보는 ‘개인을 알아볼 수 있는 (특정 개인 식별)’ 정보
  - 식별의 개념은 개인정보 개념의 핵심
  - 특정 개인을 알아볼 수 있는 정보
  - 개인을 구별하기 위하여 부여된 식별기호(특정 개인의 정체성을 나타내는 정보)
  - 개인에 대한 호칭

- 4. '다른 정보와 쉽게 결합하여' 알아볼 수 있는 정보
  - IP주소, 쿠키, 로그기록, 인터넷접속정보 등은 그 자체로는 개인을 특정하는 정보는 아니지만 쉽게 개인을 추정해낼 수 있는 특성이 있는 정보
  - 차량등록번호, 사업자등록번호 등은 개인정보가 아니지만 관계되는 특정 개인과의 정보결합을 통해 쉽게 개인을 추정해낼 수 있는 정보
  - 스마트폰과 같은 이동성을 지닌 사물의 위치정보, 가전제품, 전자기기 등 고정된 사물인터넷의 위치정보는 특정 개인과의 정보 결합을 통해 쉽게 개인을 추정해낼 수 있는 정보
- 5. 정보의 종류, 형태, 성격, 형식 등에 관하여는 특별한 제한이 없음
  - 문자, 음성, 부호, 영상 등의 정보

개인정보 분류1



- 개인 데이터 : 개인에 관한 모든 데이터
- 필명, 머리색깔, 관심사, 취미 등
- 프라이버시에 관한 정보 : 개인생활과 관련된 정보
- 위치정보, 구매이력, 검색이력, 이용이력, 교통카드 이용이력 등
- 개인정보 : 특정 개인을 식별할 수 있는 정보
- 주민등록번호, 이름 등

❖ 민감데이터 : 특정한 개인의 사상.신념.노동조합 및 정당 가입.탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보

개인정보 분류 2

- 고유식별정보
  - 그 자체로 개인을 직시하는 정보
  - 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등
  - 홍채, 지문, 정맥, 안면인식 등 바이오 정보
  - 개인신용카드번호, 계좌번호 정보 등 포함
- 개인식별정보
  - 해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보
  - 이름, 주소, 전화번호, 핸드폰번호, 이메일주소, 생년월일 등
- 제한적 본인 식별정보
  - 개인식별정보와 조합하면 부가적인 정보를 제공하는 간접 정보
  - IP주소, MAC주소, 쿠키와 같은 '자동 생성 정보' 등

개인정보 분류 3

- 개인정보
  - 현실에 존재하는 자연인으로서의, 구체적인 '개인 ' 을 식별할 수 있는 정보를 의미
  - 이름, 전화번호, 주민등록번호, 주소 등이 포함
- 가명정보
  - 실명을 천공으로 대체하거나 전화번호를 가상의 번호로 대체하는 등 개인화된 부분을 가리되, 그 속성값을 알 수 있도록 하는 정보
- 익명정보
  - 특정한 인물로 알아볼 수 있는 부분을 삭제하고 지역 통계라든가 성별 통계의 개념으로 범주화 시킨 정보

익명정보와 가명정보 사례

개인정보보호론
[2주차. 프라이버시 개념]

프라이버시 권리 개념

- “The Right to Privacy “ => “The right to be let alone” 으로 개념화

- [프라이버시 침해 유형(William Prosser)]
  - 개인의 영역 또는 사적 사항에의 침입
  - 개인의 사적 사실의 공개
  - 공중으로 하여금 특정인에 대한 오해를 유발할 수 있는 사항의 공표
  - 개인의 성명이나 초상의 영리적 사용이 있는 경우 프라이버시의 침해가 이루어진 것으로 봄

프라이버시 권리 관련 CASE STUDY

- Griswold v. Connecticut (1965)
- Katz v. United States (1967)
- Roe v. United States (1973)
- Scarfo v. United States (1999)
- Kyllo v. United States (2001)
- O'connor v. Ortega (1987)

Reasonable Expectation of Privacy

- Zone of Privacy(프라이버시 구역) 필요
  - 프라이버시를 기대할 영역이 필요하다는 것
  - 국가가 사회적 질서유지나 가치관 보호를 위해 일부영역은 간섭이 가능하나 국가가 간섭하지 못하는 영역이 있다는 것
- 이를 위한 "프라이버시에 대한 합리적인 기대" 설정
  - 미국 Privacy 보호범위
  - 즉, Privacy의 보호범위는 자신이 Privacy를 유지하려는 노력의 합리적인 결과물로 정해짐)
- Reasonable Expectation of Privacy의 두가지 개념
  - A person exhibit an actual expectation of privacy
    (자신이 프라이버시 보호를 위해 합당한 조치를 취하였는가?)
  - Society recognizes the expectation as reasonable
    (사회가 그러한 개개인의 기대를 합당하다고 받아들일 수 있는지?)

정보자기결정권

- 1971년 독일의 사회학자 니클라스 루만(Niklas Luhmann)은 '정보의 자기결정권 (Informationelle Selbstbestimmung)'을 주창
  - 독일에서는 개인의 정체성이나 인격을 위해서 자신만의 고유영역을 확보할 수 있어야 하고 이러한 과정을 통해 민주적 삶을 영위할 수 있다고 보았음
- 1983년 독일 헌법재판소가 선고한 이른바 인구조사 판결 (Volkszählungsurteil)에 의해서 정보자기결정권(Recht auf informationelle Selbstbestimmung)이라는 명칭으로 수용됨
  - 인구조사법이 규정한 인구조사가 개인의 습관, 출근 교통수단, 부업 내역, 학력 등 매우 자세한 개인정보를 국민들에게 요청하고 이렇게 수집된 정보를 행정목적으로 주 정부들과 공유할 수 있도록 한 것은 헌법에 위배된다고 결정

프라이버시 권리 개념의 변화

- 전통적 의미의 프라이버시: (소극적 개념) 홀로 있을 권리(the right to be let alone), 사생활 비밀유지와 자유
- 현대적 의미의 프라이버시: (적극적 개념)
  정보프라이버시(information privacy), 개인정보 자기결정권
  - (열람, 정정 또는 삭제 요구 가능) 청구권적 기본권

➢ 광범위한 개념으로 확장: 자유로운 자기 결정권

프라이버시 개념 범위 확장

- 공간 프라이버시
  - 물리적 개념, 심리적 개념을 포함한 공간, 특히 한 개인의 지역적 독거
  - 원치 않는 대상이나 신호에 의한 침해로부터의 보호와 관련
- 결정 프라이버시
  - 프라이버시를 선택과 관련한 것으로 인식
  - 아무런 방해 없이 중요한 결정을 할 수 있게 하는 개인의 능력. 개인의 자유와 연관
- 정보 프라이버시
  - 개인정보의 흐름과 관련
  - 개인정보의 획득, 공개, 사용 등 정보처리과정에서 개인의 통제. 그리고 개인정보를 통제하기 위한 개인의 청구

프라이버시 ≠ 사생활

- 프라이버시(privacy)는 개인에 관한 정보를 다른 사람들에게 선택적으로 공개할 수 있는 권리
- 사생활 (私生活) 은 개인의 정보를 공개하지 않고 보호하는 측면을 강조
- 프라이버시는 개인의 정보를 공개 또는 비공개할 수 있는 선택적 권리를 의미
- 그런 점에서 '사생활'보다는 '프라이버시'가 좀 더 적극적인 개념

개인정보보호론
[3주차. 프라이버시원칙]

세부적인 프라이버시 개념 유형 : 6가지 유형

- 홀로 있을 권리(The right to be let alone)
  - 일반법적인 권리로서 보호해야 할 신체적, 정신적으로 "침해당하지 않은 인격"
- 접근제한(Limited access to the self)
  - 타인에 의한 원치 않는 접근을 스스로 차단할 수 있는 능력
- 기밀성(Secrecy)
  - 타인으로부터 특정 문제를 숨김(concealment)
- 개인정보통제(Control over personal information)
  - 자신에 관한 정보를 통제할 수 있는 능력
- 인격(Personhood)
  - 자신의 개성(personality), 특성(individuality), 존엄성(dignity) 보호
- 친밀감(Intimacy)
  - 자신의 친밀한 관계(intimate relationships)나 생활 측면에 대한 접근 제한이나 통제

프라이버시 인식의 변화

혼자 있을 권리
(Right to be let alone)

개인의 생활영역 또는 개인에 대한 지식과 개인적 생활 영역에 대한 한정된 정보로서의 인간 생활영역을 의미

개인정보자기결정권
(Self-control on Personal Information)

자신의 정보가 언제 어떻게 그리고 어느 범위까지 타인에게 전달되고 이용될 수 있는지를 스스로 결정할 수 있는 권리

[개인정보자기결정권의 기본정신]
- ✓타인에 의한 정보 수집·이용·제공에 대해 정보주체가 어느 정도 관여할 것인지는 개인정보의 성격, 수집목적, 이용형태, 처리방식에 따른 위험성 정도에 따라 다르나
- ✓적어도 정보주체의 인격적 요소인 개인정보가 타인에 의해 마음대로 처리·조작되어서는 안 된다는 것이 핵심

개인정보자기결정권(Self-control on Personal Information)

- 개인정보자기결정권 =
  "사적인 사항이 공개되는 것을 원치 않는 이익"(interest in avoiding disclosure of personal matters) +
  "자신의 중요한 문제에 대해 자율적이고 독자적으로 결정을 내리고자 하는 이익"(interest in independence in making certain kinds of important decisions)

- 개인정보자기결정권의 보호범위
  - 개인인격의 구성요소들이 전자적 형태로 기록화 됨으로써 정보주체의 총체적인 인격상이 타인의 수중에 들어가는 위험성을 사전에 차단하기 위해 요구되는 기본권

OECD 프라이버시 보호 가이드라인 : OECD 8원칙

구분	원칙	내용
1 원칙	수집제한의 원칙 Collection Limitation Principle	개인정보의 수집은 제한되어야 하고 수집하는 경우 합법적이고 공정한 절차에 따라 정보주체에 알리거나 동의를 받아야 함
2 원칙	정보정확화의 원칙 Data Quality Principle	개인정보는 그 이용목적에 부합하는 것만 수집하고 목적에 필요한 범위 내에서 정확하고 완전하며 최신이 상태를 유지해야 함
3 원칙	목적명확화의 원칙 Purpose Specification Principle	개인정보 수집 목적은 수집하기 이전 또는 당시에 명시되어야 하고 명시된 목적으로만 이용해야 함

OECD 8원칙

구분	원칙	내용
4 원칙	이용제한의 원칙 Use Limitation Principle	개인정보는 수집된 목적으로만 이용해야 하며 목적 이외로는 이용할 수 없음(단, 정보주체에게 별도 동의를 받거나 법률에 의해 허가된 경우는 제외)
5 원칙	안전확보의 원칙 Security Safeguards Principle	개인정보의 분실, 불법적인 접근, 훼손, 사용, 변조, 공개 등의 위험에 대비하여 합리적인 보호조치를 마련해야 함
6 원칙	공개의 원칙 Openness Principle	개인정보 관리자의 주소 등을 비롯하여 개인정보의 이용목적, 관련된 정책 등에 대한 내용이 포함된 공개방침이 있어야 함

OECD 8원칙

구분	원칙	내용
7 원칙	개인참여의 원칙 Individual Participation Principle	정보주체는 본인의 개인정보에 대해 확인, 열람요구, 이의제기 및 정정, 삭제, 보완 청구권을 가짐
8 원칙	책임의 원칙 Accountability Principle	개인정보 관리자는 위에서 제시한 원칙들이 지켜지도록 필요한 제반 조치를 취해야 함

OECD 8원칙에 기반한 Google 개인정보처리방침 검토

개인정보보호론
[4주차. 동의]

동의 기능

- **개인정보자기결정권이 실질적으로 이루어지는 방법은? 동의**

- **동의 방식**
  - **Opt-in(사전동의)**
    - ✓ **사전동의, 강제화로 문제 발생 vs 지나친 규제로 창의적 활용 저해**
  - **Opt-out(사후거부)**
    - ✓ **무분별한 정보 전송 피해**

동의 문제점

- 1. 동의 만능주의
  - 동의만 받으면 무엇이든지 할 수 있다
  - 정보주체의 동의로 부당한 상황을 승화시키는 것 => 동의를 통하여 정보주체의 이익 해침
- 2. 동의의 형식화
  - 동의가 아니라 그냥 클릭하는 과정
  - 청약 행위 + 승낙행위 + 의사 합치 => 청약 행위 + 승낙 행위 (의사의 합치가 없음)
- 3. 동의로의 일원화
  - 다른 '적법사유'의 사문화 => 다양성과 혁신의 저해 요인
- 4. 동의 내용의 난해
  - 읽고 이해하기 쉽지 않음

동의 관련

- "Privacy Policy" Dilemma
  - 개인정보를 보호하기 위하여 만든 프라이버시 정책(동의제도 포함)이 오히려 무의식적이고 무분별한 사용을 하게 함으로써 프라이버시를 해치게 되는 상황
    - ✓ 남발되는 고지와 무의식적 동의의 일상화 – 개인정보자기결정권(통제권) 허울
    - ✓ IoT, Bigdata, Fintech 산업에 장애요인
- Privacy Paradox
  - "Privacy Policy" Dilemma 의 일종으로 인식과 행태의 차이
  - 프라이버시 중요성에 대해서 추상적으로만 인식하고 실제로는 프라이버시 보호를 위한 구체적인 행동을 하지 않는 것을 의미

효율적 동의 확보 방안

- 약관 Infographics
- 등급제
- Privacy Profile Setting
- Consent Management Platform
- Personal Data Store

IoT 시대 개인정보보호 6대 위협

- 1. IoT로 인한 개인정보보호 위협 요소 : Privacy Divide
- 2. 동의서를 읽거나 동의에 클릭한다고 해도 실질적 동의로 보기 어려운 상황 발생
- 3. 수집목적을 벗어난 사물인터넷 수집 정보 유출 위험 커져
- 4. 사용자들의 기기 사용 행태나 습관 등의 모니터링과 유형화에 따른 침해 위험 확대
- 5. 사물인터넷 기기로부터 수집되는 빅데이터의 비식별성 유지의 어려움
- 6. 사물인터넷 기기간 자동 교환 정보 폭증에 따른 보안위험 증대

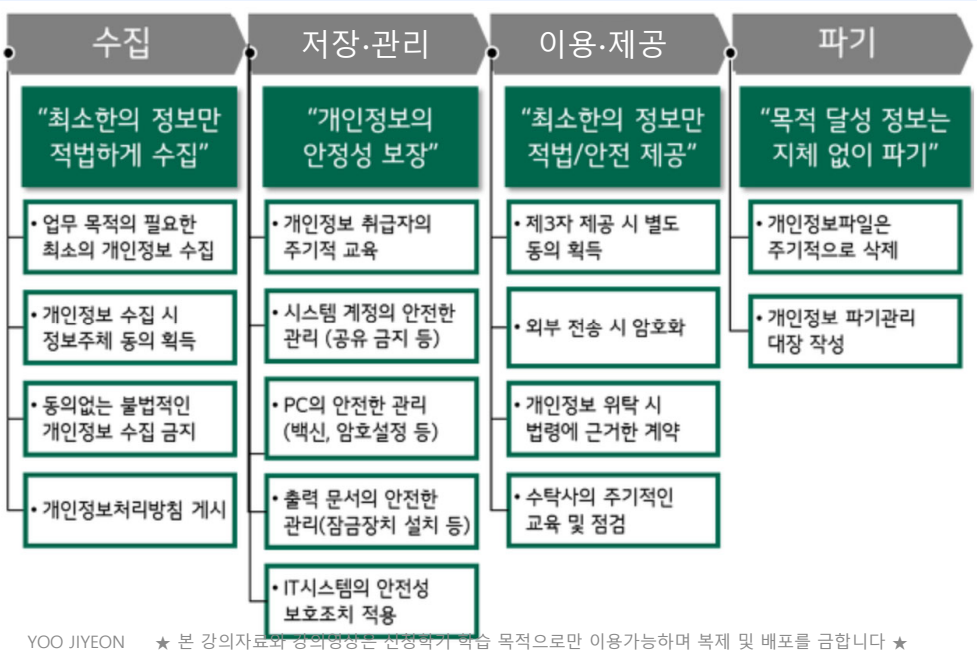
개인정보보호론
[5주차. 개인정보 생명주기]

개인정보 생명주기(Lifecycle)

- 개인정보 생명주기 : 사람의 일생처럼 개인정보 관리 단계를 의미
  - 개인정보처리자가 개인정보를 다루는 일련의 단계
  - 수집 – 저장/관리 – 이용/제공 –파기

- 개인정보 생명주기별 보안 관리모델 (TTAS.KO-12.0053)

개인정보 처리자의 의무사항

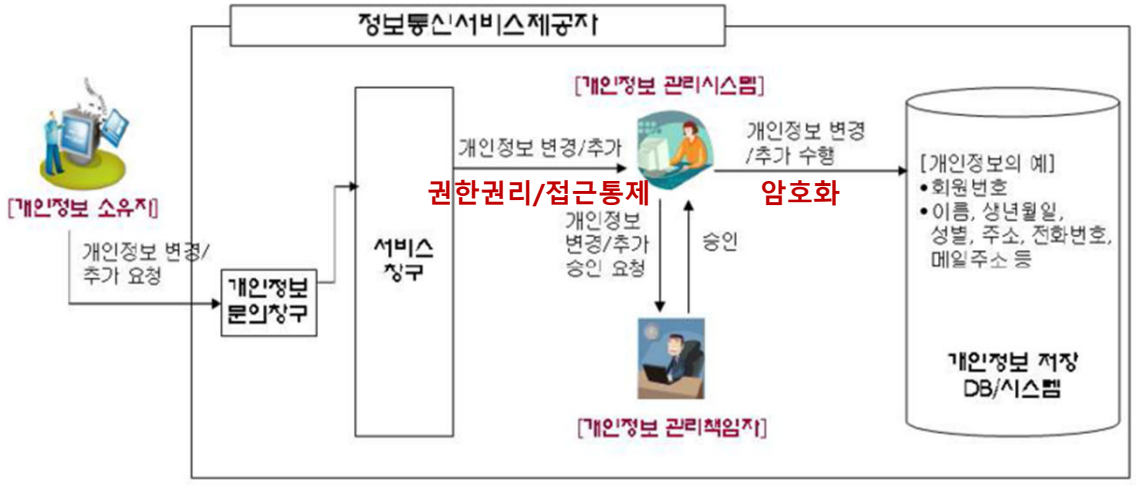


수집단계

- **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**

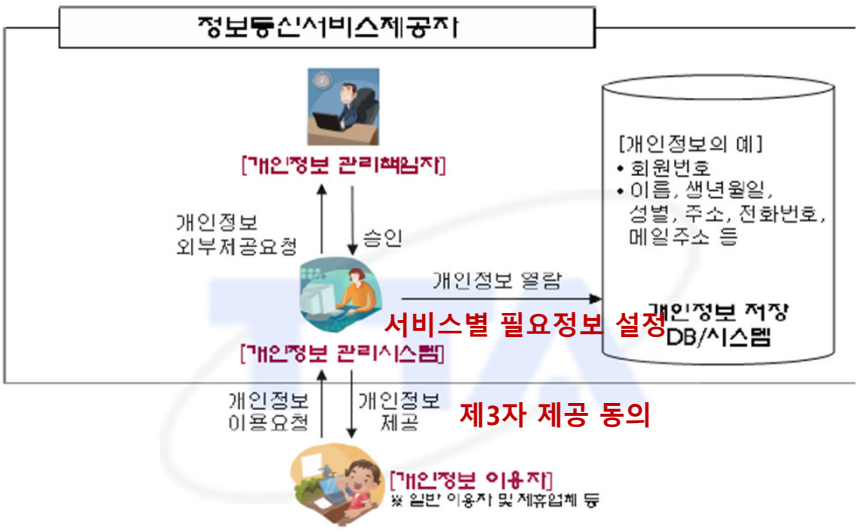
저장·관리 단계

- 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



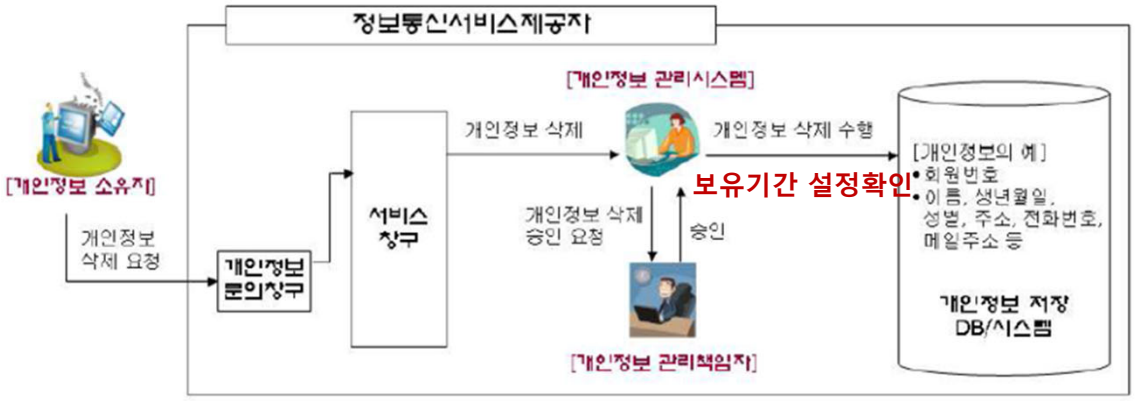
이용·제공 단계

- 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



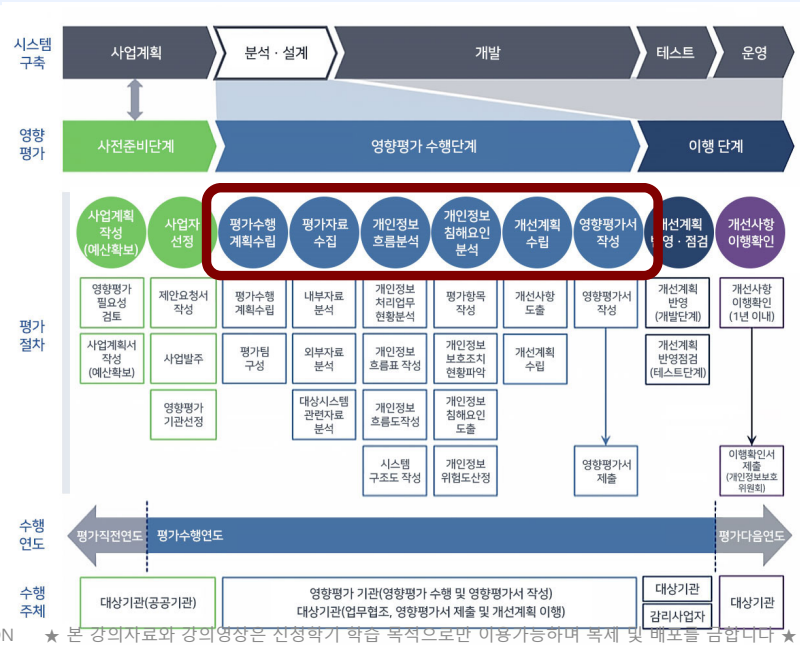
파기단계

- 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



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



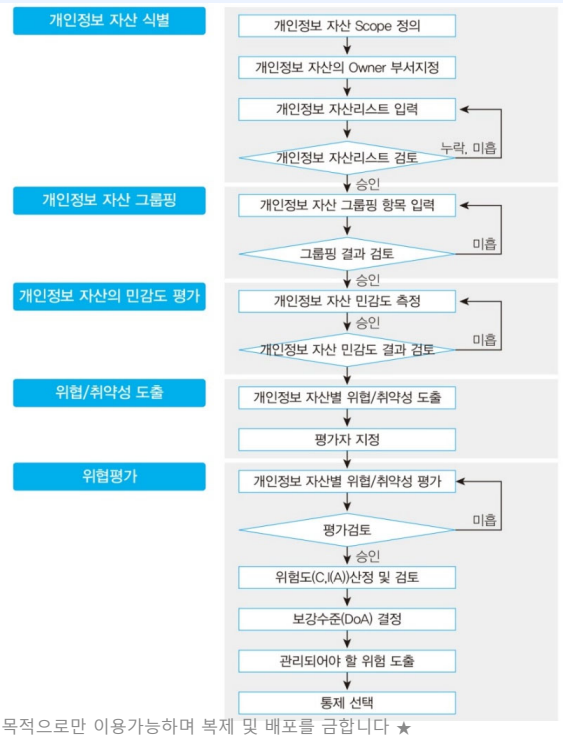
- **1. 영향평가계획 수립**
  - **평가과정에 필요한 사항들을 정리**
- **2. 평가자료 수집**
- **3. 개인정보 흐름분석**
  - **3-1. 개인정보 처리업무 현황 분석**
    - ✓ **개인정보처리 업무표 작성**
    - ✓ **개인정보 업무 흐름도 작성**
  - **3-2. 개인정보 흐름표 작성**
  - **3-3. 개인정보 흐름도 작성**
    - ✓ **1) 총괄흐름도 작성**
    - ✓ **2) 업무별 흐름도 작성**
  - **3-4 정보시스템 구조도 작성**

- 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
  - 4-2 개인정보 보호조치 현황파악(항목별 평가)
  - 4-3 개인정보 침해요인 도출
  - 4-4 개인정보 위험도 산정
    - ✓ 위험도 = 개인정보 영향도(자산가치) + (침해요인 발생가능성 X 법적 준거성) X 2
- 5. 개선계획 수립
  - 5-1 개선방안 도출
  - 5-2 개선계획 수립
- 6. 영향평가서 작성

개인정보 위험도 산정

- 위험도 = 개인정보 영향도(자산가치) + (침해요인 발생가능성 X 법적 준거성) X 2

❖ 개인정보 위험도 분석 재정리



개인정보보호론
[6주차. 안전성확보조치]

개인정보의 안정성 확보조치

▪ [제1조] 안정성 확보조치 기준의 목적

개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보에 필요한 **기술적 • 관리적 • 물리적 안전조치에 관한 최소한의 기준**을 정하는 것

▪ [제2조] 사용하는 용어

- 정보주체
- 개인정보파일
- 개인정보처리자
- 대기업
- 중견기업
- 중소기업
- 소상공인

- 개인정보보호책임자
- 개인정보취급자
- 개인정보처리시스템
- 위험도분석
- 비밀번호

- 정보통신망
- 공개된 무선망
- 모바일 기기
- 바이오정보
- 보조저장매체
- 내부망
- 접속기록
- 관리용 단말기

※용어의 정의는 고시 참조

유형별 안전조치 적용

▪ [제3조] 안전조치 기준 차등 적용

[별표] 개인정보처리자 유형에 따른 안전조치 기준 차등 적용

유형1 (완화)	1만 명 미만의 개인정보를 보유한 소상공인, 단체, 개인
유형2 (표준)	1만 명 이상의 개인정보를 보유한 소상공인, 단체, 개인 10만 명 미만의 개인정보를 보유한 대기업, 중견기업, 공공기관 100만 명 미만의 개인정보를 보유한 중소기업
유형3 (강화)	10만 명 이상의 개인정보를 보유한 대기업, 중견기업, 공공기관 100만 명 이상의 개인정보를 보유한 중소기업

내부 관리계획의 수립과 시행(제4조)

개인정보보호 내부 관리계획

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육

관리적

4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지

기술적

9. 물리적 안전조치
10. 개인정보 보호조직 구성·운영
11. 유출사고 대응계획 수립·시행
12. 위험도 분석 및 대응방안 마련
13. 재해·재난 대비 개인정보처리시스템의 물리적 안전조치
14. 개인정보처리 수탁자의 관리·감독

유형1 선택조항

15. 그 밖에 개인정보 보호를 위해 필요한 사항

물리적

내부 관리계획의 수립과 시행(제4조)

개인정보보호 내부 관리계획

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육

관리적

4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지

기술적

9. 물리적 안전조치
10. 개인정보 보호조직 구성·운영
11. 유출사고 대응계획 수립·시행
12. 위험도 분석 및 대응방안 마련
13. 재해·재난 대비 개인정보처리시스템의 물리적 안전조치
14. 개인정보처리 수탁자의 관리·감독

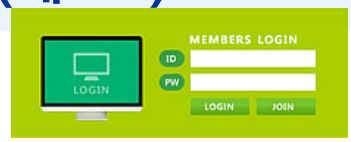
유형1 선택조항

15. 그 밖에 개인정보 보호를 위해 필요한 사항

물리적

상명대학교 SANGMYUNG UNIVERSITY
YOO JIYEON ★ 본 강의자료와 강의영상은 신청학기 학습 목적으로만 이용가능하며 복제 및 배포를 금합니다 ★

접근권한의 관리(제5조)



① 개인정보처리시스템에 대한 접근 권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여

유형1 선택조항

② 전보, 퇴직 등의 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 접근 권한을 변경 또는 말소

③ 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 3년간 보관

④ 개인정보처리시스템의 사용자계정 발급시 개인정보취급자 별로 발급하며, 다른 개인정보취급자와 공유되지 않도록 함

⑤ 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용

⑥ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근 제한 등 필요한 기술적 조치

유형1 선택조항

접근통제(제6조)

① 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 기본 조치

1. 접속 권한을 IP주소 등으로 제한 → 인가 받지 않은 접근 제한
2. 접속한 IP주소 등을 분석 → 불법적인 개인정보 유출 시도 탐지 및 대응

→ 위 기능을 포함하여 조치해야 함

IP(Internet Protocol)

② 외부에서 개인정보처리시스템에 접속하려는 경우 안전한 접속수단 또는 안전한 인증수단 적용

유형1 선택조항

※ 가상사설망 (VPN : Virtual Private Network) 또는 전용선 등

③ 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 개인정보가 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등 조치 수행

접근통제 (제6조)

④ 인터넷 홈페이지를 통해 고유식별정보가 유출. 변조. 훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치 수행 ☑ 유형1 선택조항

⑤ 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 해야 함 ☑ 유형1 선택조항

⑥ 별도의 개인정보처리시스템이 아닌 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우

- 제1항 적용 안 함
- 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능 이용 가능

⑦ 업무용 모바일 기기의 분실. 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치

개인정보의 암호화(제7조)

암호화 필요 대상 고유식별정보, 비밀번호, 바이오정보

암호화 기준

구 분				암호화 기준
정보통신망, 보조저장매체를 통한 송, 수신 시	비밀번호, 바이오정보, 고유식별정보			암호화 송, 수신 ※제7조 ①항 TIP 참조
정보처리 시스템에 저장 시	비밀번호			일방향(해쉬 함수) 암호화 저장
	바이오정보			암호화 저장
	고유식별정보	주민등록번호		암호화 저장
		여권번호, 외국인등록번호, 운전면허번호	인터넷 구간, 인터넷 구간과 내부망의 중간 지점 (DMZ)	암호화 저장
			내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부. 적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장 시	비밀번호, 바이오정보, 고유식별정보			암호화 저장(비밀번호는 일방향 암호화 저장)

- 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행 ☑ 유형1,2 선택조항
- 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장

접속기록의 보관 및 점검(제8조)

① 접속한 기록을 **6개월 이상 보관. 관리**

② **반기별로 1회 이상** 점검 → 개인정보의 **분실. 도난. 유출. 위조. 변조 또는 훼손** 등에 대응하기 위하여

③ 개인정보취급자의 접속기록이 위. 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관

접속ID, 날짜와 시간, IP주소, 수행업무

정기적으로 백업 수행

정기 점검 / 후속 조치

악성프로그램 등 방지(제9조)

악성프로그램 등을 방지. 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치. 운영해야 함

1. 보안 프로그램은 항상 최신의 상태로 유지

- 자동 업데이트 기능 사용
- 일 1회 이상 업데이트 실시

2. 악성프로그램 관련 경보 발령 또는 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트 실시

3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

관리용 단말기의 안전조치(제10조)

개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로
개인정보처리시스템에 직접 접속하는 단말기

1 인가 받지 않은 사람이 임의로 조작하지 못하도록 조치

2 본래 목적 외로 사용되지 않도록 조치

3 악성프로그램 감염 방지 등을 위한 보안조치 적용

물리적 안전조치(제11조)

① 개인정보 보관을 위한 물리적 보관 장소(전산실, 자료보관실 등)는 출입통제 절차를 수립. 운영

② 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관

③ 개인정보가 포함된 보조저장매체의 반출. 입 통제를 위한 보안대책을 마련

다만, 별도의 개인정보처리시스템 없이 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우는 예외

재해·재난 대비 안전조치(제12조)

유형1,2 선택조항

화재, 홍수, 단전 등의 재해. 재난 발생 시

① 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검

② 개인정보처리시스템 백업 및 복구를 위한 계획 마련

개인정보의 파기(제13조)

① 개인정보 파기 조치

1. 완전파괴(소각. 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 1항의 방법이 어려울 경우 일부 파기 조치

전자적 파일	개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
기록물, 인쇄물, 서면, 그 밖의 기록매체	해당 부분을 마스킹, 천공 등으로 삭제

기술적 안전성 확보 조치 종합