보다나은 정부	보 도 자 료	작성과	개인정보보호정책과
행정안전부	2018년 10월 17일(수) 조간 (10. 16. 12:00 이후)부터 보도하여 주시기 바랍니다.	담당자	과 장 김상광 사무관 소진숙
		연락처	02-2100-3480 02-2100-4091

중소기업 개인정보 유출 사전예방 위한 새로운 지침 만든다

- 행정안전부, 「시스템 개발자용 개인정보보호 적용 가이드」 개발 -

□ **행정안전부**(장관 김부겸)는 시스템 개발단계에서부터 **중소기업의 개인정보 유출 취약점**을 사전에 **예방·제거**하기 위해 시스템 구축 방법론과 개인정보 처리흐름을 결합한 **「시스템 개발자용 개인정보보호 적용가이드」**를 개발한다.

□ 이번 지침서는 중소기업의 누리집(홈페이지) 서비스 개발과 운영·관리를 담당하는 **시스템 구축업체를 대상**으로 하여 전문성과 재원이 부족한 **중소기업을 지원**하기 위하여 **발간**하게 되었다.

※ 중소사업자가 전체 사업자(3,459,437개)의 약 98%를 차지('17년 개인정보보호 실태조사)

※ 개인정보 유출사고 발생의 주요 원인 중, 인터넷 홈페이지 취약점이 약 60% 차지

○ 중소기업의 **누리집·앱 서비스 등 개발·운영관리**는 대부분 시스템 구축(SI, System Integration)업체에 **의존**하고 있고, **개인정보 유출사고** 대부분이 **SI업체**가 운영 중인 경우에 발생하고 있어 지침개발 필요성이 지속적으로 제기되어 왔다.

○ 특히 시스템개발자 스스로 개발 全과정에 걸쳐 **개인정보보호 방법론**을 사전에 **적용**하는 방식(**프라이버시 보호 설계**, PbD)을 안내한다.

※ 프라이버시 보호 설계(PbD, Privacy by Design) : 시스템 기획단계에서부터 폐기 단계까지에 걸쳐 이용자의 프라이버시와 데이터 보호를 위한 정책 및 기술

□ 가이드는 **개인정보 생애주기**에 따라 지켜야할 의무·권고사항을 **시스템 구축 단계별**로 유형화하여 제시한다.

< 시스템 구축 단계별 개인정보 생애주기에 따른 준수사항 >

구분	기획 단계	개발 단계	운영 단계
수집	• 제공하려는 서비스 유형 • 서비스에 필요정보 종류	• 수집 시 동의 획득 구현 • 수집 시 최소화 구현	• 추가된 개인정보 수집 항목 • 서비스 유형 변경
저장·보관 이용·제공	• 개인정보 암호화 방식 • 제3자 제공, 연계 여부	• 접속기록 자동화	• 개인정보처리방침 현행화 • 내부관리계획 현행화
파기	• 보관기간·파기방안 마련	• 파기 자동화	• 과거 수집한 주민등록번호 파기 수행

○ 먼저, **개인정보 생애주기**(수집, 저장·보관, 이용·제공, 파기)와 **시스템 구축단계**(기획, 개발, 운영)에 따라 필요한 **안전조치 방안을 안내**한다.

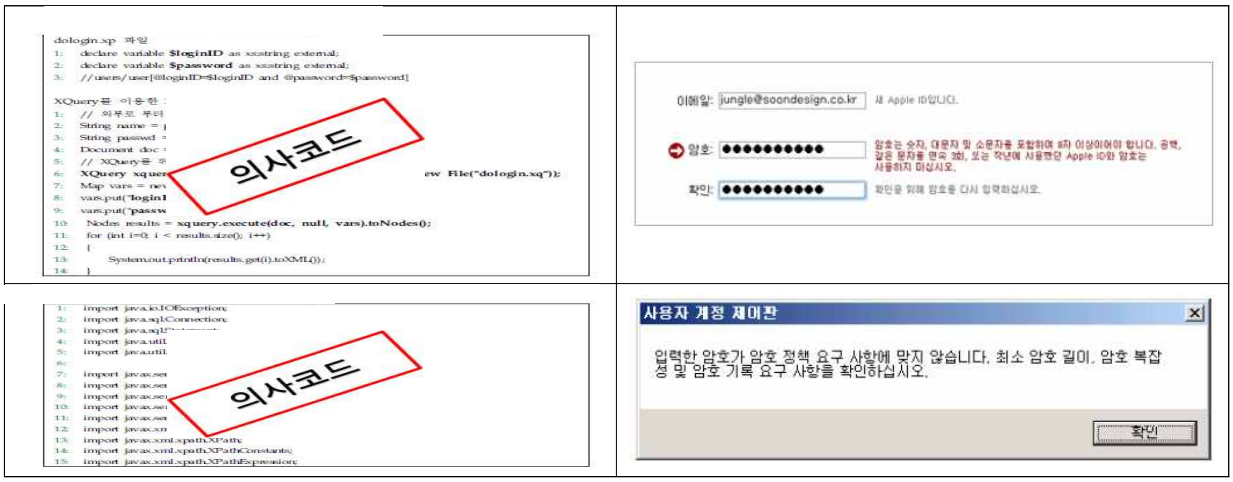
- 시스템 **기획단계**에서는 개인정보 수집 최소화 방법, 고유식별정보, 민감정보 등 중요 개인정보의 암호화 알고리즘 방식 등을 제시한다.
- 시스템 **운영단계**에서는 목적을 달성한 개인정보에 대한 기술적·관리적인 파기 자동화방법 등을 제공한다.

○ 또한, **개인정보 처리흐름**(예: 정보주체 동의획득→정보입력→암호화전송)을 도식화하고 안전조치 방안을 **법적 의무사항·권고사항**으로 **유형화**하여 제시한다.

- **의무사항**은 개인정보처리자가 반드시 준수해야할 사항으로, 예를 들어 개인정보처리자는 누리집을 통한 회원등록을 할 수밖에 없는 경우 주민등록번호를 사용하지 않고 회원을 받을 수 있는 방안을 마련하여야 한다. 주민등록번호 수집은 법률·대통령령에 근거가 없는 경우에는 고객동의에 의해서도 수집이 금지된다.
- **권고사항**은 개인정보 안전성 조치 강화를 위한 적용방안을 제시함으로써 시스템 개발자가 자율적으로 조치하도록 권장한다. 예를 들면, 개인정보 수집·이용 동의함에 기본 값 미 설정 조치, 안전한 인증수단(로그인) 구현방법 등을 제시한다.

○ 더불어, 안전조치 유형화, 도식화에 따른 **개발보안 코딩, 암호화 조치** 등 안전조치 구현 방법을 개발한다.

<개인정보 생애주기 코딩과 적용화면 예시 >



□ 이를 통해 시스템개발자가 직접 개인정보보호 방법을 숙지하여 시스템 기획·분석·설계·구축·운영 단계에서 **사전에 침해요인을 제거**함으로써 개인정보를 유출을 예방할 수 있을 것으로 기대된다.

○ **안전한 인증수단**(로그인) 등 외부 접근통제 방법이나 암호화 코딩 방법을 제공하므로 누리집 취약점으로 인해 발생할 수 있는 해커 공격을 막을 수 있음은 물론,

○ **접속기록 자동화 방법**을 제공함으로써 개인정보를 접근하는 사람·시점·접근 내용·다운로드 횟수를 자동으로 생성하여 개인정보 유출을 사전에 예방할 수 있다.

□ **정윤기 전자정부국장**은 “이번 시스템 개발자용 개인정보보호 적용 가이드 발간으로 취약점을 사전에 제거하고, 특히 전문성과 재원이 부족한 **중소기업의 개인정보 관리에 큰 도움이 될 것**으로 기대한다.” 라고 말했다.

붙임 | **가이드개발내용 예시: 홈페이지 위반사례, 조치방법 안내**

[위반사례 1]

○ C회사는 온라인으로 회원관리 중이다. 이를 위하여 회원가입을 위한 개인정보 수집·이용 동의를 회원가입자로부터 받고 있다.

C회사가 제공한 동의화면은 개인정보 수집목적, 수집항목, 보유·이용기간을 알리고 동의란 체크박스로 구성되어 있다.

이는 정보주체에게 개인정보 수집·이용 관련 필수 고지사항 4가지 중 '동의거부 권리와 동의거부에 따른 불이익'에 대해서는 전혀 고지하지 않아 불완전한 형태의 동의이다.

이 경우 회원 가입자는 동의거부 권리와 거부에 따른 불이익에 대한 사전안내가 없기 때문에 제한된 선택을 할 수밖에 없고 자신의 권리를 침해당한다.

위반내용(Before)	조치방법(동의할 때 4가지 고지)
동의거부 권리와 거부에 따른 불이익 누락된 동의 화면	수집항목과 수집목적, 보유기간, 거부권과 불이익
	

[위반사례 2]

○ 주민등록번호는 법령 등에 수집근거가 있어야 처리가능하고 ①과거에 저장·보관한 주민등록번호라도 수집근거가 없다면 즉시 삭제해야한다.

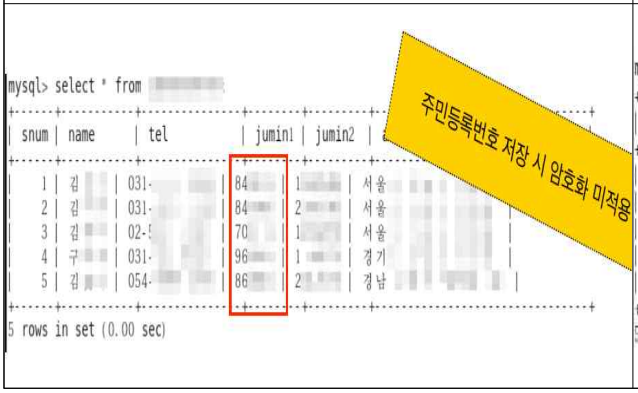
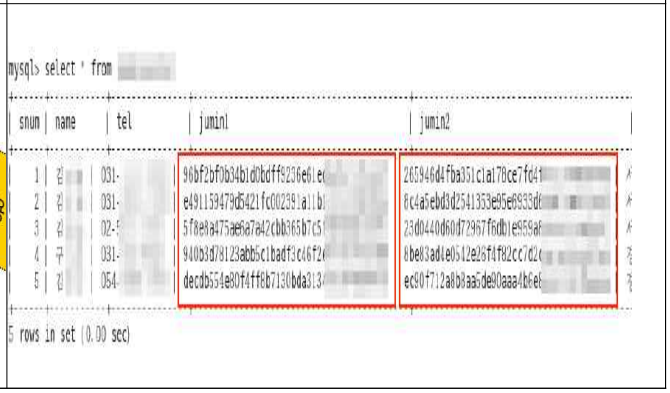
○ 홍씨는 교육훈련 국비지원을 받기위해 A학원에 등록하면서 자신의 주민등록번호*를 포함한 개인정보를 기입하였다.

* 노동부에서 제공하는 교육훈련 국비지원으로 무상교육을 받을 수 있음

A학원은 이렇게 수집한 학원생의 개인정보 중 주민등록번호를 개인정보처리시스템에 저장하여 이용·관리하고 있다.

A학원 개인정보처리시스템은 학원생 주민등록번호에 대하여 암호화를 적용하지 않아 13자리 번호가 모두 노출된 채 저장·관리되고 있는 것으로 드러났다.

주민등록번호는 고유식별정보로 반드시 안전한 암호 알고리즘을 사용하여 ②암호화 적용하여 저장·관리하여야 한다.

위반내용(Before)	조치방법(주민등록번호 암호화 또는 파기)
①법령근거 없이 수집했던 주민등록번호 보관	법령근거 없이 수집했던 주민등록번호 파기조치
123456-1234567	update [table_name] set jumin2 = null delete jumin2 from [table_name] alter table [table_name] drop column jumin2
②주민등록번호 저장 시 암호화 미적용	주민등록번호 저장 시 암호화
	

[위반사례 3]

○ B학원은 외국어 학원 홈페이지와 유학관련 홈페이지에서 회원으로 가입한 고객정보 수집·저장을 위해 2개의 개인정보처리시스템을 운용중이다.

개인정보처리시스템은 개인정보취급자의 접속기록을 전혀 보관·관리하고 있지 않았다.

모든 개인정보처리시스템은 개인정보취급자 접속기록에 대하여 필수항목 4가지[①계정(ID), ②접속일시, ③접속자정보(IP 주소), ④수행업무]를 정확하게 기록해야한다.

B학원과 같은 개인정보처리자는 접속기록을 최소 6개월 이상 안전하게 보관·관리하며, 접속기록 이상 유무를 정기적으로 점검하여야 한다.

위반내용(Before)	조치방법(접속기록 4항목 보관·관리)
접속기록 보관·관리 소홀	접속기록 최소 6개월 이상 보관·관리·점검

번호	일자	시간	계정(ID)	아이피	
5	2013-11-02	10:30:10		192.168.1.10	직원조회
6	2013-11-02	10:31:07		192.168.1.10	고객관리 조회
7	2013-11-02	11:15:50		192.168.1.10	프로그램 시작
12	2017-02-08	10:22:15		192.168.1.10	데이터 수정
13	2017-02-08	10:23:01		192.168.1.10	직원조회
14	2017-02-08	10:24:05		192.168.1.10	프로그램 종료

[위반사례 4]

○ **oo구청이 암호화 등 보호조치를 하지 않아 홈페이지에서 신분증, 통장정보 등 개인정보가 유출되었다.**

민원인이 구청 홈페이지 **게시물 인터넷주소를 임의로 변경**하여 본인확인 없이도 타인의 장애인등록증(사진 등 비정형정보) 등 **첨부파일이 그대로 노출**

※ (접속주소) http://www.ooo.go.kr/file=0183
(임의변경) http://www.ooo.go.kr/file=0185
⇨ 타인의 신분증 사진 열람 가능

▪ **재발방지 대책으로는**

① 홈페이지 등에서 자료 접근 시 로그인 등 **외부 접근통제를 강화하고,**

② **고유식별정보가 포함된 파일은 반드시 암호화**하여 관리

⇨ 가이드에서는 안전한 인증수단(로그인) 등 외부 접근통제 방법이나 암호화 방법에 대한 코딩방법을 제공한다.

○ 개인정보를 유출한 개인정보처리자에 대한 침해사고 예방을 위한 행태를 살펴보면

① 개인정보 수집이 그다지 필요하지 않은 기업체나 소상공인 등은 아예 수집·활용의 절차를 없앴다.

② 회원가입을 소셜 로그인(네이버, 카카오 등)으로 전환했다.

③ 개인정보보호나 보안 일체를 신뢰성 있는 업체에 수탁했다.

⇨ 시스템 개발 SI업체는 개인정보 수집·보관을 줄이는 이러한 사례를 민간, 공공기관 개인정보처리자가 실정에 맞게 적용할 수 있도록 안내한다.