

개인정보보호 위반사례 및 대응



1. 실태점검 위반사례

개인정보보호법
시행 5년
- 아직도 절반은

(단위 : 건수)

개인정보보호법 관련 법조항	2015년		2014년		2013년	
(제15조) 개인정보 수집 동의 및 고지	30	12.4%	24	12.7%	36	14.7%
(제21조) 보유기간 경과 개인정보 미파기	19	7.9%	7	3.7%	9	3.7%
(제22조) 구분동의(마케팅등) 받는 방법 미흡	21	8.7%	14	7.4%	16	6.5%
(제26조) 필수항목 포함된 문서로 미계약	36	14.9%	43	22.8%	61	24.9%
(제29조) 안전성 확보 조치 미흡	68	28.1%	91	48.1%	104	42.4%
(제30조) 처리방침 필수항목 누락 공개	26	10.7%	1	0.5%	9	3.7%



3. 법규 위반 사례 분석 - 수집

개인정보 수집·이용
정보주체 동의가 필요

시민게시판, 민원신고센터 등 개인정보 수집 시,
개인정보 수집·이용 동의 절차 누락

제15조(개인정보의 수집·이용)제1항제1호

- 01 개인정보의 수집·이용 목적
- 02 수집하려는 개인정보의 항목
- 03 개인정보의 보유 및 이용 기간
- 04 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

※ 반드시 필요한 항목과 부가적인(선택) 항목을 구분하여 고지



개인정보수집 및 이용

게 수집,이용목적
공급계약서 작성, 시설분담금 부과, 도시가스 사용량 검침, 사용요금 관련 업무처리, 고객불만사항처리, 기타 관리사항 동의 정보제공 및 도시가스 사업법에 따른 안전관리 업무 처리

나 수집하는 개인정보의 항목

1) 필수항목 : 성명, 주소, 연락처(일반전화번호, 휴대전화번호), 회사홈페이지 ID/비밀번호

다 개인정보의 보유/이용기간 : 동의시점 ~ 사용계약 종료 후 5년까지
-> 법정관리정보 수집의 동의를 받음 때에는 기간의 동의 사항을 구분하여 고지(이용자)이

위 내용에 동의 하십니까? ☒ 예, 동의 합니다. ☐ 아니요 동의하지 않습니다.

[참고] 동의를 받을 때는



Check



최소한의 개인정보만 수집하여야 하며,
동의 받을 땐 **동의 사항을 구분**하여
정보 주체가 **명확하게 인지**할 수 있도록
안내하고 **각각 동의를** 받아야 한다



개인정보 수집·이용 동의서

- 정보주체의 동의를 받아 개인정보를 수집하는 경우

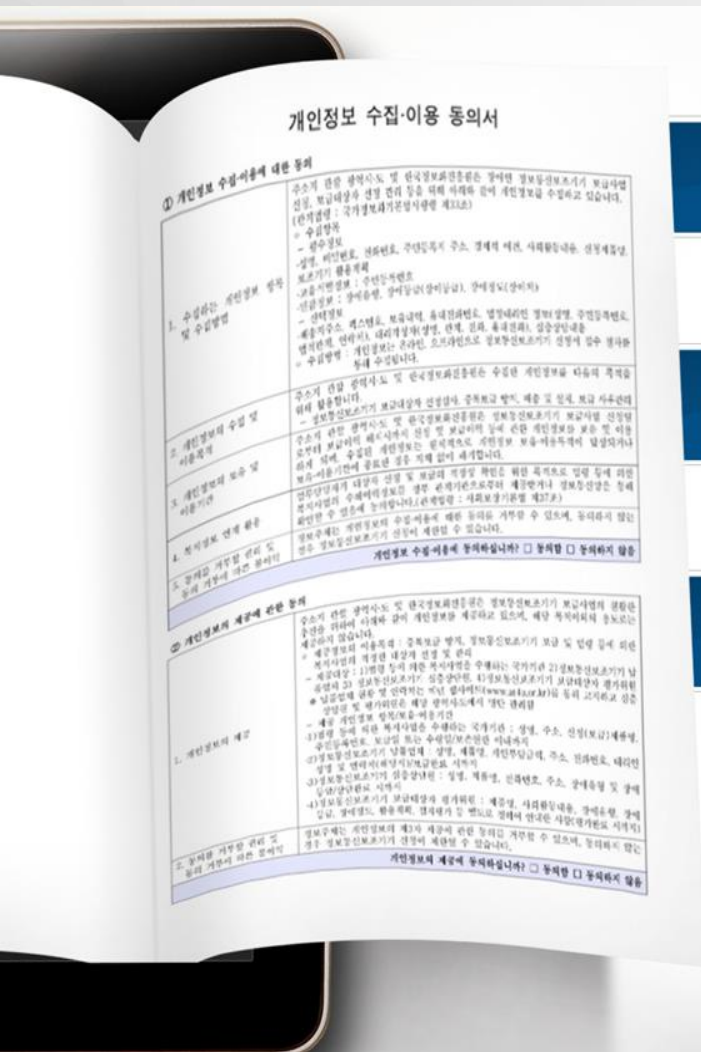
- 정보주체의 동의를 받아 제3자에게 제공(공유)하는 경우

- 제15조제1항, 제17조1항의 목적을 초과하여 이용·제공하는 경우

- 재화나 서비스를 홍보하거나 판매를 권유 동의

- 14세 미만 아동의 개인정보를 처리하기 위해 법정대리인의 동의를 받는 경우

[참고] 동의가 필요한 경우



제23조(민감정보의 처리 제한)제1호

- 민감정보를 수집하거나, 제3자에게 제공하는 경우

제24조(고유식별정보의 처리 제한)제1항

- 고유식별정보를 수집하거나, 제3자에게 제공하는 경우

제24조의2(주민등록번호 처리의 제한)

- 주민등록번호 처리를 원칙적으로 금지하고, 예외적인 경우에만 허용

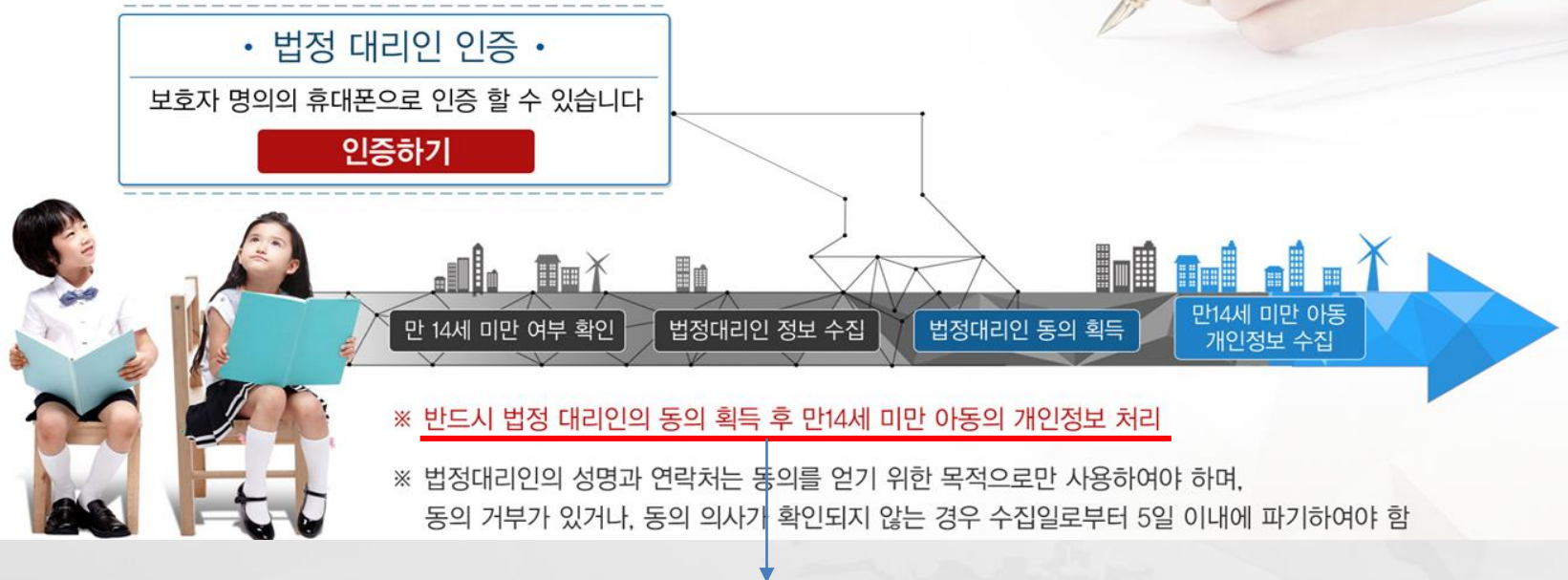
- 01 법령(법률·시행령·시행규칙)에서 구체적으로 주민번호 처리를 요구·허용한 경우
- 02 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위해 명백히 필요한 경우
- 03 기타 주민번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우

※ 현재 보유 주민등록번호는 법 시행 후 2년 이내('16년.8.6.까지) 파기

3. 법규 위반 사례 분석 - 동의

| 제22조(동의를 받는 방법)제5항

- 만14세 미만 아동의 개인정보를 처리하기 위해 법정대리인의 동의를 받는 경우 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 함



어린이·청소년 도서관 홈페이지 등에서
회원 가입시 부모 동의절차 누락

3. 법규 위반 사례 분석 - 파기

제21조(개인정보의 파기)



개인정보를 수집 시 보유 및 처리기한을 구체적으로 안내

※ “처리목적 달성 시”와 같이 목적의 구체적인 내용을 알 수 없는 표현 사용하지 않음

보유기간, 처리목적 달성, 서비스의 폐지, 사업의 종료 등 불필요하게 되었을 경우 **5일** 이내에 개인정보를 파기

법령에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우는 **다른 정보와 분리**하여 저장·관리하여야 한다

※ 법령에 따라 분리 저장·관리 시 법령에서 요구하는 개인정보 항목만을 구분하여 별도 저장·관리

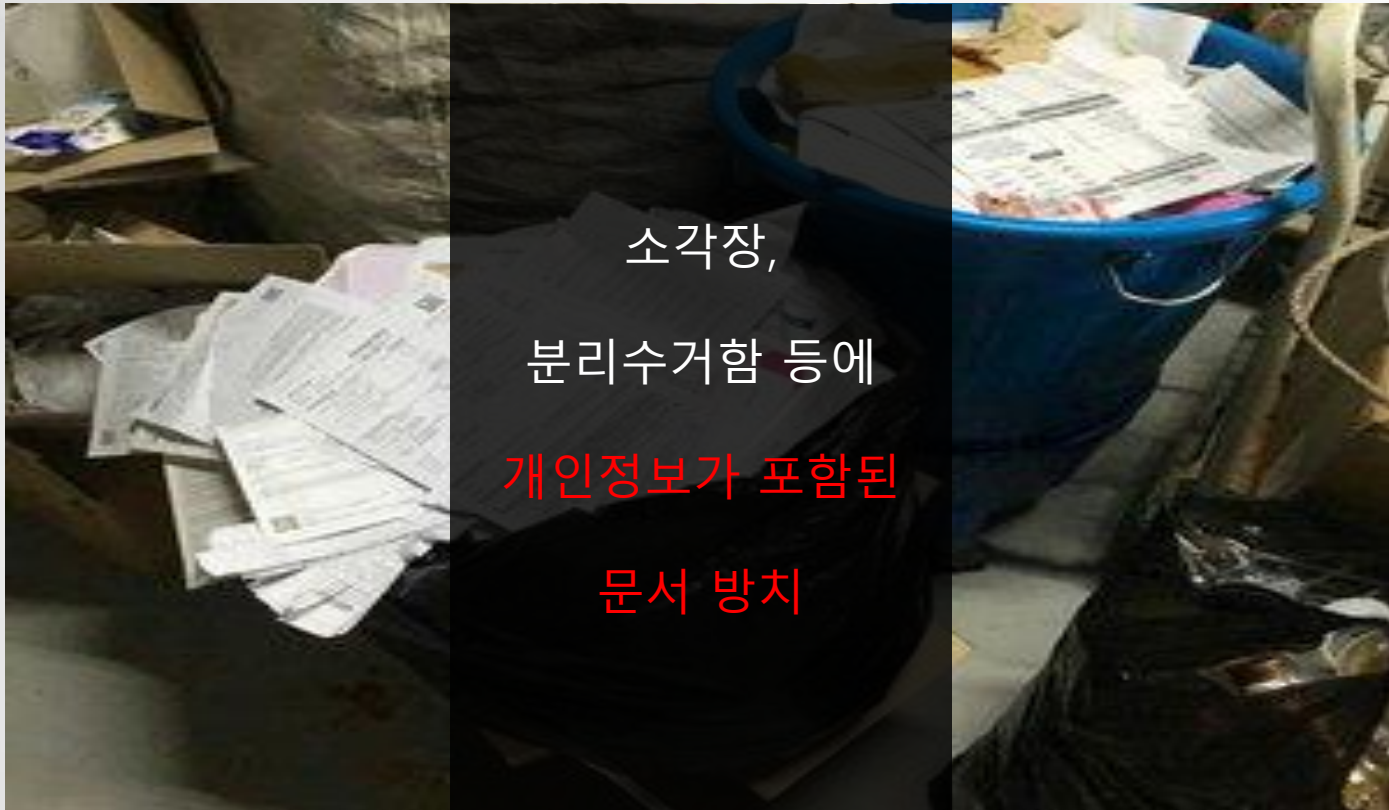
제24조의2(주민등록번호 처리의 제한) ①제24조1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외 하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

⇒ 기존에 동의를 기반으로 수집한 주민번호는 이미 파기 완료해야 함('16.8.7)

⇒ 개정된 법령에 따라 기존에 수집한 주민번호는, '17.3.29일 이전까지 파기해야 함

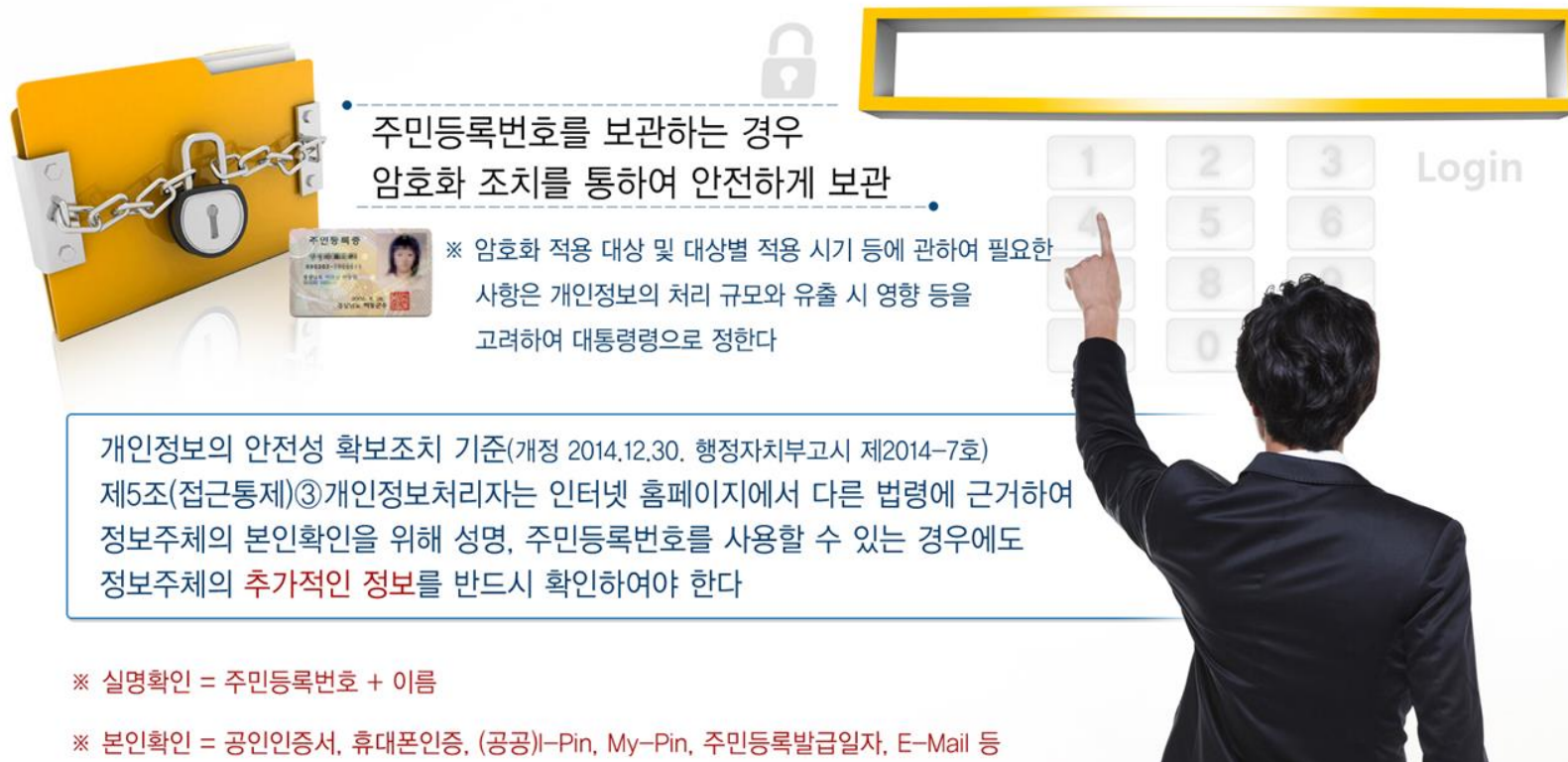
3. 법규 위반 사례 분석



3. 법규 위반 사례 분석 – 주민등록번호 처리

| 제24조의2(주민등록번호 처리의 제한)

- 법령에 따라 주민등록번호를 처리하는 경우에도 인터넷 홈페이지를 통해 회원으로 가입하는 단계에서는 **주민등록번호를 사용하지 아니하고도** 회원으로 가입할 수 있는 **방법을 제공**하여야 한다



주민등록번호를 보관하는 경우
암호화 조치를 통하여 안전하게 보관

※ 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다

개인정보의 안전성 확보조치 기준(개정 2014.12.30. 행정자치부고시 제2014-7호)
제5조(접근통제)③개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 **추가적인 정보**를 반드시 확인하여야 한다

※ 실명확인 = 주민등록번호 + 이름

※ 본인확인 = 공인인증서, 휴대폰인증, (공공)I-Pin, My-Pin, 주민등록발급일자, E-Mail 등

3. 법규 위반 사례 분석 - 업무위탁

| 제26조(업무위탁에 따른 개인정보의 처리 제한)제1항

- 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다

01

위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

02

개인정보의 기술적·관리적 보호조치에 관한 사항

03

위탁업무의 목적 및 범위

04

재위탁 제한에 관한 사항

05

개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항

06

위탁업무와 관련하여 보유하고 있는
개인정보의 관리 현황 점검 등 감독에 관한 사항

07

법 제26조제2항에 따른 수탁자가 준수 하여야 할 의무를 위반한
경우의 손해배상 등 책임에 관한 사항

개인정보
위탁 처리



3. 법규 위반 사례 분석 - 업무위탁

제26조(업무위탁에 따른 개인정보의 처리 제한)제4항

- 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리 하는지를 감독하여야 한다

수탁자 선정

수탁자를 선정할 때에는 인력과 물적 시설, 재정 부담능력 등을 종합적으로 고려하여야 한다

수탁자 처리 업무 지연

개인정보처리자는 수탁자의 처리 업무의 지연, 처리 업무와 관련없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련해야 하여야 한다

위탁 개인정보 보호

수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준」에 따라 관리적·기술적·물리적 조치를 하여야 한다



3. 법규 위반 사례 분석

개인정보 처리 업무 위탁 Vs 제3자 제공

업무 위탁

- 제26조
- 배송업무 위탁, TM 위탁 등
- 정보주체가 사전 예측 가능
(정보주체의 신뢰 범위 내)
- **원칙** 위탁사실 공개
예외 위탁사실 고지(마케팅 업무 위탁)
- 위탁자 책임
- 위탁자 부담(사용자 책임)

관련조항

예시

예측 가능성

이전방법

관리·감독 책임

손해배상 책임

제3자 제공

- 제17조
- 사업제휴, 개인정보 판매 등
- 정보주체가 사전 예측 곤란
(정보주체의 신뢰 범위 밖)
- **원칙** 제공목적 등 고지 후
정보주체의 동의 획득
- 제공받는 자 책임
- 제공받는 자 부담

※ 개인정보처리시스템의 개발·유지보수, 웹호스팅 서비스 제공 등도 업무 위탁

3. 법규 위반 사례 분석 - 안전조치

제29조(안전조치의무)

- 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다



※ 출처 : 개인정보의 안전성 확보조치 기준 [시행 2014.12.30.] [행정자치부고시 제2014-7호, 2014.12.30., 일부개정]

3. 법규 위반 사례 분석 - 접근통제

- 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가 받지 않은 접근을 제한 하여야 한다

※ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다

- 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인 정보 유출 시도를 탐지하기 위한 조치를 하여야 한다



접근통제

- 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN) 또는 전용선등 안전한 접속수단 적용 하여야 한다



- 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 이용하는 경우에도 정보주체의 추가적인 정보 (i-PIN, 공인인증서, 휴대전화, 주민등록증 발급일자, 전자우편(e-mail) 주소 등의 수단)를 반드시 확인하여야 한다

② 외부에서 접속시 VPN 등 안전한 접속수단 적용 또는 안전한 인증수단 적용

3. 법규 위반 사례 분석 - 접근권한/접속기록

접근권한의 권리



- 01 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소
- 02 권한의 부여·변경 또는 말소에 대한 내역을 기록하고 최소 3년간 보관
- 03 개인정보취급자별로 계정 발급 및 계정 공유 금지
- 04 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행 할 수 있도록 비밀번호 작성규칙을 수립하여 적용

· 최소 10자리 이상 : 영대문자(A~Z), 영소문자(a~z), 숫자(0~9), 특수문자(32개) 중 **2종류** 이상으로 구성
· 최소 8자리 이상 : 영대문자(A~Z), 영소문자(a~z), 숫자(0~9), 특수문자(32개) 중 **3종류** 이상으로 구성

⑥ 개인정보취급자가 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근 제한

접속기록의 보관 및 점검



- 01 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다
- 02 개인정보처리자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리 시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다
- 03 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다

3. 법규 위반 사례 분석 - 암호화

| 제29조(안전조치의무)

개인정보의 암호화(고유식별정보, 비밀번호, 바이오정보)

- 01 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송·수신 하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화 하여야 한다
- 02 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다 단, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다
- 03 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다

※ 주민등록번호는 구간에 관계없이 2016.1.1.부터 암호화해야 한다

- 100만 이상 : 2018.1.1까지
- 100만 미만 : 2017.1.1까지



```

[HTTP request 1/3]
[Response in frame: 13]
[Next request in frame: 15]
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "mode" = "login"
    Key: mode
    Value: login
  Form item: "contentUid" = "9be517a74fa674f8014faad5c63302bd"
    Key: contentUid
    Value: 9be517a74fa674f8014faad5c63302bd
  Form item: "contentView" = "contentView"
    Key: contentView
    Value: contentView
  Form item: "returnUrl" = "/index.9is"
    Key: returnUrl
    Value: /index.9is
  Form item: "userId" = "testjy"
    Key: userId
    Value: testjy
  Form item: "userPassword" = "test1234!"
    Key: userPassword
    Value: test1234!
  
```



⑥ 안전한 **암호키 관리**(생성, 이용, 보관, 배포, 파기 등)에 관한 절차 수립·시행

3. 법규 위반 사례 분석 – 개인정보 처리방침

개인정보 처리방침의 공개

- 개인정보 처리방침을 수립하거나 변경하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재
- 「개인정보 처리방침」이라는 명칭을 사용하되 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분



- 사업장등의 보기 쉬운 장소에 게시
- 관보(공공기관), 사업장 등이 있는 시·도 이상의 지역을 주된 보급 지역으로 하는 일반일간신문, 일반주간신문 또는 인터넷신문
- 같은 제목으로 연 2회 이상 발행되어 정보주체에게 배포하는 간행물, 소식지, 홍보지 또는 청구서 등
- 재화나 용역을 제공하기 위하여 정보주체와 작성한 계약서

홈페이지를 운영하지 않거나
관리상의 하자가 있는 경우

[참고] 개인정보 처리방침 - 필수 기재사항

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리 · 의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항
 - 처리하는 개인정보의 항목
 - 개인정보의 파기에 관한 사항
 - 제30조에 따른 개인정보의 안전성 확보 조치에 관한 사항

4. 개인정보 유출이란?



- 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보 처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 경우

01

- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용컴퓨터 등을 분실 또는 도난당한 경우

02

- 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

03

- 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우

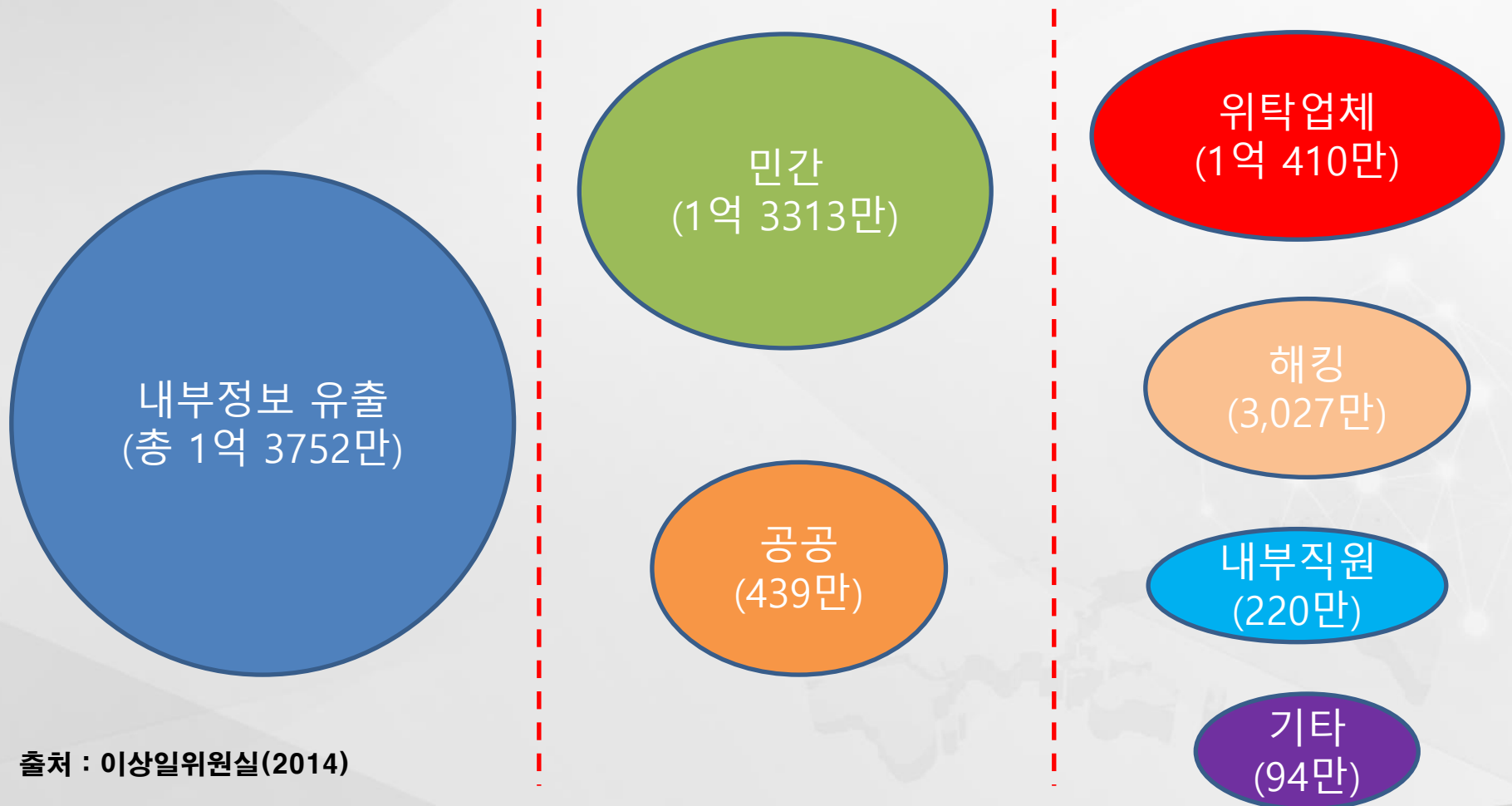
04

- 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우



6. 왜 개인정보 유출이 발생하는가?

관리소홀 탓 개인정보 유출, 해킹보다 3배 높다!!!



[참고] SQL Injection

- 웹 응용 프로그램에 강제로 SQL구문을 삽입하여 내부 DB서버의 데이터를 유출 및 변조하고 관리자 인증을 우회

id:

pw:

Login

id:

pw:

Login

id:

pw:

Login

자유 게시판

본 게시판은 로그인후 이용할 수 있습니다.

아이디

패스워드

[확인](#) [회원가입](#)

관리자님 [내정보](#) [로그아웃](#)

[me](#) | [메일 137](#) | [쪽지 1](#) | [MY서비스](#)

[알림](#) [구독](#) [메일 137](#) [카페](#) [블로그](#)

select id from [table_name] where id='admin' and pw=""

< 그림 출처 : 인터넷 >

[참고] 웹셸 (Web Shell)

- 웹페이지의 웹(Web)과 서버에 명령을 내려 실행하기 위한 인터페이스 역할을 하는 셸(Shell)의 합성어
 - 원격에서 웹 서버에 명령을 수행할 수 있도록 작성한 웹 스크립트 파일
- 해커가 작성한 웹셸을 정상적인 파일로 위장해 웹 서버에 업로드 한 후, 대상 서버에 접근해 개인정보 유출, 악성코드 유포 등 공격 수행



웹셸 악용 피해사례



6. 왜 개인정보 유출이 발생하는가?

✓ 무단제공 및 사적 열람이 **전체의 약 80%**

● 기관 유형별 (단위 : 명)

구분	중앙행정기관	교육기관	지방자치단체	기타공공기관	계
'12년	28	20	32	8	88
'13년	83	17	42	12	154
'14년	98	9	48	13	168

약 2배 증가

● 징계 유형별 (단위 : 명)

구분	파면	해임	강등	정직	감봉	견책	경고등	계
'12년	2	4	0	7	15	8	52	88
'13년	4	6	0	12	21	36	75	154
'14년	1	3	1	20	27	65	51	168

● 위반 내용별 (단위 : 명)

구분	무단 제공	외부 유출	사적 열람	단순 노출	기타	계
'12년	39	4	21	15	9	88
'13년	33	5	68	4	44	154
'14년	58	2	71	11	26	168

출처 : '공공기관의 개인정보 오·남용 징계 현황', 행정자치부

공무원이 주민 1500명 개인정보 유출

f t ↗ ★ ☰

+ -

평창 미탄면 9급, 이장에 명부 줘
군 "감사 끝나면 중징계할 방침"

공무원이 지역 주민 1500여명의 개인정보를 유출해 물의를 빚고 있다.



7. 유출된 후에는 어떻게 해야 하는가?

01

신속 통지

▶ 유출된 정보주체 개개인에게 지체 없이 통지

| 시 한 | 유출되었음을 알게 되었을 경우 지체 없이(5일 이내)

- | 통지항목 |
- 1 유출된 개인정보의 항목
 - 2 유출 시점 및 그 경위
 - 3 피해 최소화를 위한 정보주체의 조치방법
 - 4 기관의 대응조치 및 피해구제 절차
 - 5 피해 신고 접수 담당부서 및 연락처

02

긴급 조치

▶ 피해 최소화 위한 대책 마련 및 필요한 조치 실시

| 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등
피해를 최소화하기 위해 필요한 긴급 조치 이행

| 긴급 조치 이행 등에 어려움이 있는 경우 전문기관에 기술지원 요청

03

대량 유출

▶ 1만 명 이상 유출된 경우 유출 통지 결과를 신고하고 홈페이지에 공지

| 1만 명 이상 개인정보가 유출된 경우 유출 통지 및 조치 결과를 지체 없이
행정자치부 또는 전문기관(한국인터넷진흥원, www.privacy.go.kr)에 신고

| 1만 명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을
인터넷 홈페이지에 7일 이상 게재

8. 개인정보 노출이란?

일반적으로 홈페이지를 이용하는 자(이하 홈페이지 이용자)가 **해킹 등 특별한 방법을 이용하지 않고**, 정상적으로 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 **인터넷에 방치되어 있는 것**

**XX보험사 고객정보 70만건
인터넷에 노출**

**구글에 떠 있는 개인정보
이력서에 인감증명까지...**

**구글 해킹에 취약한
웹 페이지들...**

8. 개인정보 노출 현황

구 분	노출 사이트 수	노출건수	구분			
			중앙부처	지자체	기 타	사업자
13년	727	56,226	1,048	18,863	20,723	15,592
14년	687	130,264	1,629	26,045	15,394	87,196
15년	774	182,445	509	6,623	32,903	142,410



엑셀파일에 의한 노출

[숨기기] 기능에 의한 개인정보 노출

공시송달

합수 치환 후 원본 내용 미삭제로 인한 개인정보 노출

이미지파일에 의한 노출

개인정보가 담긴 이미지 파일(JPG, GIF, BMP, PNG 등)에 의한 노출

개인정보가 담긴 이미지형 PDF 파일에 의한 노출

개인정보를 회원 식별자로 사용

개인정보가 담긴 이미지형 PDF 파일에 의한 노출

< 주요 개인정보 노출사례 유형 >

9. 노출사고를 예방하려면?

이용자 주의사항

게시판에 글을 올릴 때는
**개인정보가 있는지 반드시
확인 후 삭제**하세요.



꼭 필요한 개인정보는
마스킹 처리 후 업로드하세요.

성명	주민등록번호	휴대폰
홍+홍	123456-1	010-△△△△△-1234
김+홍	123456-2	010-△△△△△-2345
박+일	123456-3	010-△△△△△-5678

개인정보가 포함된 게시글은
비밀글로 설정하세요.



운영자 주의사항

게시판 운영 시 **개인정보
노출주의에 대해** 안내하세요.

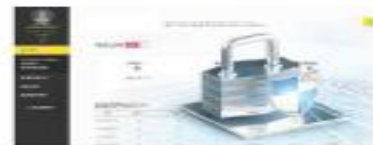
개인정보 게시에 대한 주의안내

게시판 내용 입력 및 첨부파일업로드 시 개인정보가 포함된 경우
개인정보가 노출되어 악용될 수 있으니 주의하시기 바랍니다.

FAQ

질문	답변
1. Q. 개인정보가 포함된 게시글을 업로드할 수 있는 방법?	A. 1. 개인정보가 포함된 게시글을 업로드할 수 있는 방법
2. Q. 개인정보가 포함된 게시글을 삭제할 수 있는 방법?	A. 2. 개인정보가 포함된 게시글을 삭제할 수 있는 방법
3. Q. 개인정보가 포함된 게시글을 수정할 수 있는 방법?	A. 3. 개인정보가 포함된 게시글을 수정할 수 있는 방법
4. Q. 개인정보가 포함된 게시글을 검색할 수 있는 방법?	A. 4. 개인정보가 포함된 게시글을 검색할 수 있는 방법
5. Q. 개인정보가 포함된 게시글을 삭제할 수 있는 방법?	A. 5. 개인정보가 포함된 게시글을 삭제할 수 있는 방법

**관리자페이지는
안전하게 보호**하세요.



- 관리자페이지의 주소에 추측가능한 단어 (admin, manager 등) 사용 자제하기
- 관리자만 접속할 수 있도록 IP 제한하기
- 외부접속이 필요한 경우 전용선이나 가상사설망(VPN) 이용하기

홈페이지의 **개인정보
노출여부를 점검**하세요.



- 검색사이트에 내가 처리하는 개인정보가 있는지 점검하기
- 홈페이지 변동(통합, 개선) 시 점검하기
 1. 회원 식별자로 개인정보 쓰지 않기
 2. 웹 취약점 진단하기
 3. 시큐어 코딩 준수하기

Internet On, Security In!

감사합니다

