2013 개인정보 보호를 위한
데이터베이스 보안 세미나

IBM

2013 개인정보보호법의 이해와 대비

한국IBM 정보관리사업부
신경미 (kmshin@kr.ibm.com)

개인 정보 보호와 개인 정보 보호법의 기본 원칙

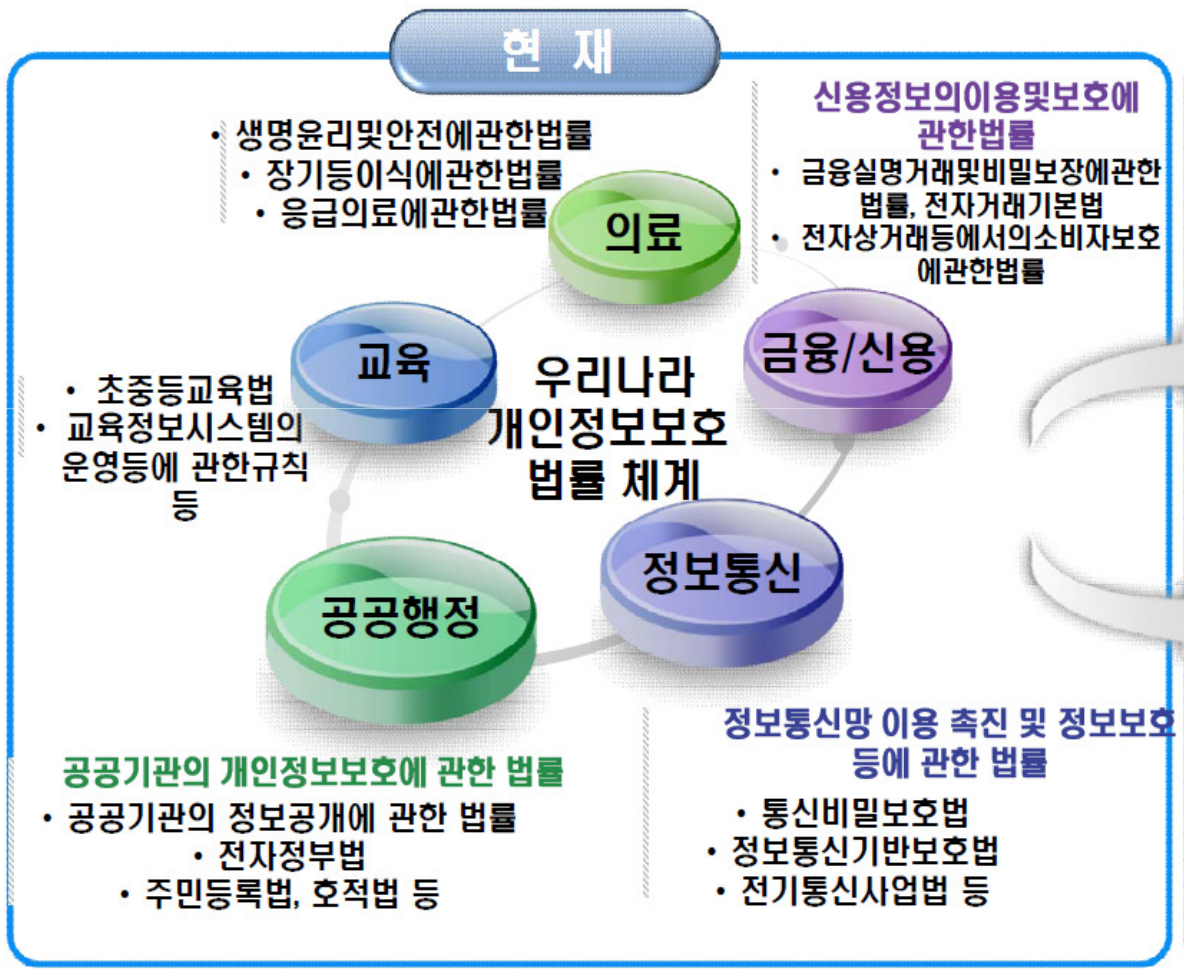
개인 정보 보호란?

- 개인 정보의 수집, 이용 과정에서 정보 주체의 동의를 받는 등 **정당하게 개인 정보를 수집 및 이용** 해야 한다.
- 개인 정보의 보관, 관리 과정에서 **내부자의 고의 및 부주의 또는 외부 공격으로부터 유출, 변조, 훼손** 되지 않도록 해야 한다.
- 개인 정보의 파기, 삭제 과정에서 **정보 주체의 개인 정보가 자기 결정권이 제대로 행사될** 수 있도록 보장하는 일련의 행위 및 조치이다.

개인 정보 보호법의 기본 원칙

- 목적에 필요한 최소한 범위 내에서 **적법하고 정당하게 수집해야** 한다.
- 처리목적 범위 내에서 **정확성, 완전성, 최신성을** 보장해야 한다.
- 처리 목적의 **명확화가** 이루어 져야 한다.
- 필요 목적 범위 내에서 **적법하게 처리, 목적 외 활용을 금지해야** 한다.
- 정보 주체의 권리 침해 위험성 등을 고려 하여 **안전성을 확보해야** 한다.
- 개인 정보 처리 사항을 **항상 공개** 되어야 한다.
- 열람청구권 등 **정보주체의 권리는 보장** 되어야 한다.
- **개인정보처리자의 책임 준수 및 실천, 신뢰성이 확보** 되도록 노력해야 한다.

컴플라이언스 대응: 개인정보보호법 제정



개인정보 보호법
(법률 제10465호)
- 2011년 3월 29일 제정
- 2011년 9월 30일 시행!

살아 있는 개인에 관한 정보로서
성명, 주민등록번호(고유 식별 번호) 및 영상 등을 통하여 개인을 알아볼 수 있는 정보.
(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다.)

2012년 개인정보 보호 주요현황(1/3)

12년 침해 유형 및 실태

개인정보 생명주기	침해 유형	118 신고 (166,801건)	분쟁조정 (143건)	행정처분 (756건)
수집	• 이용자의 동의 없는 개인정보 수집 • 과도한 개인정보 수집, 민감한 개인정보 수집 • 주민등록번호 수집방법 위반, 도용/침해	- 3,507건 - 847건 -139,724건	- 19건 - 1건 -	- 111건 - 46건 - 53건
관리	• 기술적 · 관리적 조치 미비로 개인정보 침해 • 위탁절차 위반 및 위탁업체 관리감독 미흡	- 3,855건 - 125건	- 17건 -	- 103건 - 28건
이용 제공	• 목적 외 이용 및 동의없는 제3자 제공 • 접근권한 부실, 부당 공유 및 불법 거래 • 개인정보 이용 동의 철회 및 회원탈퇴 요구 불응	- 2,196건 - 941건 - 1,377건	- 76건 - 2건 - 2건	* 검거 / 기소 - 1건 - 3건
파기	• 정당한 이유없는 개인정보 보유 및 미파기	- 779건	- 10건	- 6건
기타	• 개인정보처리방침 누락, 미공개 등	- 12,915건	- 16건	- 124건

출처: 안행부 개인정보보호 정책방향 (2013.06)

2012년 개인정보 보호 주요현황(2/3)

12년 실태점검 및 처분현황

총 47회 756개소 점검, 과태료 57건, 시정조치 360건 등 총 441건 행정처분

구분	금융업	학원	협회/연맹	공공기관	운송업	의료업	기타	전체
점검기관	37	25	25	74	27	21	232	441
위반기관	33	20	17	49	17	11	217	364
위반비율	89.2%	80.0%	68.0%	66.2%	63.0%	52.4%	93.5%	82.5%

조사 및 점검

-기획 점검 : 취약 분야, 위험 업종 대상 중심 실시, 제도개선 병행 (정기)

-특별 점검 : 침해사고, 유출 신고 등 사고 원인조사 및 책임 규명 (수시)

<개인정보보호 합동점검단>

현황 조사분석
- 업종별 개인정보처리현황
- 개인정보관리실태
- 개인정보 제공/활용현황

▶ KISA, NIA, 리서치 등

모니터링
- 개인정보 유/노출현황
- 온라인 점검 (취약점 분석)

▶ 관계부처/기관 연계

침해사고, 민원
- 개인정보 침해신고, 민원
- 분쟁조정 신청
- 사고 발생, 언론 보도 등

▶ 경찰, KISA 등

출처: 안행부 개인정보보호 정책방향 (2013.06)

2012년 개인정보 보호 주요현황(3/3)

대규모 개인정보 침해사례

발생일	피해규모	발생기업	사고원인
2011.06	1,900만 건	대부업체	해커가 고객정보 유출 후 인터넷에서 거래
2011.07	3,560만 건	포탈업체	해커가 관리자 ID/비밀번호를 탈취
2011.09	80만 건	카드업체	자사직원이 유출
2011.11	1,320만 건	게임업체	해킹
2012.04	1,175만 건	인터넷쇼핑몰	운영자가 고객정보를 마케팅 업체에 유출
2012.05	400만 건	교육 미디어	해킹
2012.07	877만 건	통신업체	고객정보조회시스템 해킹

출처: 안행부 CPO역할의 과제 (2013.06)

실태진단 결과 중점 개선 필요사항

< 개인정보처리시스템 관리 >

안전성 확보조치 및 관리를 위한 접근권한 관리, 접속기록 정기점검 등 수행

접근권한 및 접속기록

접근권한 관리

- 책임자 : 전체권한 부여
  예) 읽기, 쓰기, 변경
- 취급자 : 업무 목적에 따라 최소한의 범위로 부여 예) 읽기

차등부여

- 전보, 퇴직 등 인사이동 시 해당 계정을 변경 및 말소

권한삭제

- 접근권한 부여, 변경, 말소에 대한 내역 기록 및 보관(3년)

이력관리

접속기록 관리

정기점검, 후속조치

- 사용자별 수행한 명령기록
- 사용자의 접속상태
- 사용자들의 정보(로그인, 로그아웃, 재부팅) 등 점검
- 불법적인 접근방지를 위한 대책마련 등 후속조치 이행

기록관리

- 접속 ID, 날짜 및 시간, IP주소, 수행업무 등을 저장(6개월이상)
- 정기적으로 백업을 수행

출처: 안행부 개인정보보호 정책방향 (2013.06)

개인정보 보호법 개정안 의결 (2013년 9월 30일), 2014년 8월부터 시행–

개인정보에 대한 기술적 보호 조치 (개인정보 – 고유식별정보 에 대한 암호화 조치) 의무화에 대한 준수 및 기업의 가장 소중한 자산인 고객정보(DB)에 대한 유출 통제 및 차단 방안 마련이 필요

구분	현행	개정안
주민등록번호 수집이용	정보주체의 별도동의, 법령에 구체적인 근거가 있는 경우 수집 이용	**주민등록번호 원칙적 처리금지 및 법 시행 2년 내에 파기해야 함** **단,예외적용:** **-법령에 구체적인 근거 있는 경우** **-정보주체 또는 제3자의 급박한 생명,신체,재산의 이익을 위해 명백히 필요한 경우** **-안전행정부령으로 정하는 경우**
과징금 제도	없음	**주민등록번호 분실,도난,유출,변조,훼손 시** **최대 5억원 과징금 부과** **단, 안전성 확보조치를 모두 이행한 경우 제외**
CEO 징계권고	개인정보 법규 위반 시, 책임 있는 자를 징계할 것을 그 소속 기관 단체 등의 장에게 권고	**책임 있는 자에 해당 기관 대표자 및 책임 있는 임원이 포함된다는 것을 명확화**

개인정보의 안전성 확보조치 기준

구분	주요내용
내부관리계획 수립·시행(제3조)	• 보호책임자 지정 및 역할과 책임, 취급자 교육 등
접근권한 관리(제4조)	• 업무수행에 필요한 최소한의 범위로 차등 부여 • 접근권한 부여기록은 최소 3년간 보관
비밀번호 관리(제5조)	• 비밀번호 작성규칙 수립 의무화
접근통제시스템(제6조)	• 방화벽 등 접근통제시스템 설치 · 운영 • 업무용 컴퓨터만을 이용해 개인정보 처리시, 접근통제시스템 설치의무 면제 (O/S, 보안프로그램의 접근통제기능 이용)
암호화(제7조)	• 암호화 대상 : 고유식별정보, 비밀번호, 바이오정보 • 암호화 기준 -(전송시) 정보통신망 송수신 등의 경우 암호화 -(저장시) ① 비밀번호 및 바이오정보 암호화 (비밀번호 일방향 암호화) ② 고유식별정보는 인터넷구간, DMZ구간 저장시 암호화하고 내부망 저장시 위험도 분석에 따라 암호화 적용여부, 적용범위 결정
접속기록 보관(제8조)	• 최소 6개월 이상 보관
보안프로그램(제9조)	• 백신 등 보안프로그램 설치, 자동 또는 일1회 이상 업데이트
물리적 접근방지(제10조)	• 개인정보 물리적 보관장소에 대한 출입통제절차 등

미조치에 따른 유출시	벌칙조항	2년 이하 징역 또는 1천만원 이하 벌금
보호조치 미비	벌칙조항	3천만원 과태료

개인정보 보호법 안전성 확보조치 주요 위반 사례 및 벌칙

개인정보보호책임자 및 개인정보취급자외 자에게 개인정보처리 시스템에 대한 접근 권한 부여 사례

⇒ 개인정보보호책임자 및 개인정보취급자에 한하여 시스템접근권한을 부여하여야 함 (제29조, 시행령 제30조제1항2호)

⇒ 안전조치를 위반하여 개인정보를 분실. 도난. 유출. 변조 또는 훼손당한 경우에는 2년 이하의 징역 또는 1천만 원 이하의 벌금에 해당(제73조제1호)

* 감사원 감사 시 인사이동 등에 의한 **시스템 접근권한 만료자의 접근권한 삭제 미조치 지적

외부망에서 개인정보처리시스템에 접속이 필요한 경우에 안전한 인증수단 미적용 및 방화벽, IDS, IPS, WAF 등 개인정보에 대한 불법적인 접근을 차단하기 위한 접근통제시스템 미설치 사례

⇒ 개인정보처리자는 침해사고 방지를 위한 접근통제 등을 시행하고, 보안프로그램(백신) 등을 설치하여야 함(제29조, 시행령 제30조제1항2호)

개인정보 및 인증정보 송. 수신 시 보안서버 미구축 사례

⇒ 개인정보처리자는 침해사고 방지를 위해 개인정보 및 인증정보 송・수신시 보안서버를 구축(암호화 전송)하여야 함(제29조, 시행령 제30조제1항3호)

* 암호화 대상 정보 : 고유식별정보, 바이오정보, 비밀번호

DB 접근 내역을 확인 할 수 있는 로그 기록의 6개월 이상 보관 관리 기준 미충족 사례

⇒ 개인정보처리자는 개인정보처리시스템 접속 기록 6개월 이상 보관. 관리하여야 함(제29조, 시행령 제30조제1항4호6호)

개인정보보호법 의무사항 및 위반 시 벌칙표

개인정보 안전관리	개인정보의 누설 또는 타인 이용에 제공(제59조)	5년 이하 징역 또는 5천만원 이하 벌금
	개인정보의 훼손, 멸실, 변경, 위조, 유출(제59조)	
	CCTV 설치목적과 다른 목적으로 임의 조작하거나 다른곳을 비추는 자 또는 녹음기능을 사용한 자(제25조)	3년 이하 징역 또는 3천만원 이하 벌금
	직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자(제60조)	
	안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자(제24조, 제25조, 제29조)	2년 이하 징역 또는 1천만원 이하 벌금
	안전성 확보에 필요한 조치의무 불이행(제24조, 제25조, 제29조)	3천만원 이하 과태료
	CCTV 설치·운영기준 위반(제25조)	
	개인정보를 분리해서 저장·관리하지 아니한 자(제21조)	1천만원 이하 과태료
	개인정보처리방침 미공개(제30조)	
	개인정보보호책임자 미지정(제31조)	
	CCTV 안내판 설치 등 필요조치 불이행(제25조)	

개인정보 침해로 인한 기업의 손실 및 사례

- 개인정보 침해로 기업은 아래와 같이 손실을 보게 됩니다.
  - **기업 이미지에 심각한 타격**
  - **대규모 손해 배상 책임**
  - **회사와 임직원에 해당 징계 및 제재**
  - **형사 책임**

회사 및 발생 시기	유출된 개인정보	법원의 결정	1인당 배상액	진행 상황
N소프트 (2005.5)	게임 접속자 5명의 아이디, 비밀 번호	아이디와 비밀 번호는 개인 정보에 해당	3명에게 1인당 10만원	2009년 6월 대법원 확정
K은행 (2006.5)	32,000여 명의 고객이름, 주민등록번호, 이메일 무단 전송	인격적 이익 침해로 인한 정신적 손해배상 인정	1024명에게 1인당 10만원 ~ 20만원	2007년 11월 항소심 확정
L전자 (2006.9)	입사지원자 290여명의 자기소개, 경력, 학력정보 해킹으로 유출	자기소개서 정보는 아이디보다 보호가치 높다	자료 조회된 32명에 1인당 70만원, 나머지는 30만원	2008년 11월 확정
A사 (2008.2)	해킹으로 1081만 명의 회원 이름, 아이디, 주민등록번호 등 노출	개인정보 유출이지만 A사측의 개인정보 관리 상의 과실 부정	1인당 50 ~ 300만원 청구(패소)	

현재 H캐피탈, S카드, N포탈 등을 상대로 집단 소송 중

개인정보보호법 상담사례집 FAQ

Q1> 회사에 고객들의 이름, 주소, 전화번호, e-mail, 비밀번호를 저장하고 있습니다. 암호화 대상이 무엇인가요?

A> 개인정보의 안전성 확보조치 기준 고시 제7조에서 암호화 대상은 고유식별정보 (주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오 정보입니다. 따라서 이 경우에 현재 기준으로는 비밀번호만 일방향 암호화해서 저장하시면 됩니다.

Q2> 개인정보의 안전성 확보조치는 무엇인가요?

A>개인정보 처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 다음과 같은 기술적·관리적 및 물리적 조치를 강구해야 합니다.

1. 관리적 조치 : 내부관리계획의 수립 및 시행, 교육계획 수립 및 실시, 기록물의 관리및 보호조치, 정기적인 자체 감사의 실시, 보호(보안)구역 지정 등
2. 물리적 조치 : 출입통제 장치 설치, 물리적 잠금장치 설치, 감시장치 설치 등
3. 기술적 조치 : 시스템 접근권한 관리, 접근권한 확인(식별, 인증 등), 침입차단, 방지시스템 설치, 고유식별정보의 암호화, 접속기록의 위변조 방지, 보안프로그램의 설치, 주기적인 S/W업데이트 및 점검 등

Q3> 개인정보보호법 시행으로 개인정보보호 의무를 지는 대상, 즉 적용대상 및 범위가 달라지나요?

A> 개인정보보호법 시행 이전에는 개별법이 있는 경우에 한해 개인정보보호 의무가 있었습니다.

※ 공공기관(공공기관의 개인정보보호에관한법률), 정보통신서비스제공자 및 준용사업자(정보통신망 이용촉진 및 정보보호 등에 관한 법률), 신용정보 제공·이용자(신용정보의 이용 및 보호에 관한 법률).

개인정보보호법 시행 이후, 공공·민간부문의 모든 개인정보처리자가 적용대상이 됩니다. 즉, 제조업, 서비스업 등 72개 업종 320만 전체 사업자 대상이며, 중앙행정기관은 물론 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관과 협회·동창회 등 비영리단체도 대상이 됩니다.

개인정보보호법 상담사례집 FAQ

Q4> 개인정보처리시스템을 위탁하거나, ASP(Application Service Provider)를 이용하는 경우 암호 수행을 위탁기관에서 해야 하는지 아니면 수탁기관에서 해야 하는지?

A> 개인정보의 암호화 등 안전성확보조치는 원칙적으로 "개인정보처리자"의 의무입니다. 따라서 개인정보처리시스템을 위탁하거나 ASP를 이용하는 경우에도 암호화 조치사항에 대한 이행여부에 대한 책임은 위탁기관이 지게 됩니다.

다만, 위탁기관은 암호화에 대한 요구사항을 수탁기관과의 계약서 등에 명시하여 수탁기관으로 하여금 처리하게 요구할 수 있습니다.

Q5> 주민등록번호를 저장하면 무조건 암호화해야 하나요?

A> 필요성 판단 후 암호화 합니다. 인터넷에서 직접 접근이 가능한 구간(인터넷망, DMZ 구간)에 위치한 시스템에 저장하면 암호화해야 하나, 물리적인 망분리, 방화벽 등으로 분리된 내부망에 저장하면 개인정보 영향평가나 위험도 분석을 통해 필요한 경우에만 암호화를 합니다.

만일, 전용선을 이용하여 개인정보를 송·수신하는 경우, 암호화가 필수는 아니나 내부자에 의한 개인정보 유출 등을 대비해서 가급적 암호화 전송을 권장하고 있습니다. 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 개인정보 영향평가 및 위험도 분석결과에 따라 암호화 적용여부 및 적용범위를 결정하여 시행할 수 있습니다.

즉, 시행령 제38조에 따라 영향평가의 대상이 되는 공공기관은 해당 개인정보 영향평가의 결과에 따라 암호화의 적용여부 및 적용범위를 정하여야 하며, 개인정보 영향평가의 실시대상이 아니거나 공공기관 이외의 개인정보처리자는 위험도 분석을 실시한 후 그 결과에 따라 고유식별정보의 암호화 적용여부 및 적용범위를 정하여 시행합니다.

Q6> 국내에 있는 직원의 DB가 해외 시스템에 있는데 암호화를 해야 하나요?

A> 해외 시스템에 DB가 있다고 하더라도 국내의 법률을 준수하여야 합니다. 따라서 개인정보제공자 및 수신자, 수신한 자로부터 개인정보를 재차 수령한 제2의 개인정보 처리자는 개인정보가 이전되는 과정 또는 이전된 이후 개인정보가 불법열람, 유출 등 침해가 발생 되지 않도록 적절한 수준의 기술적·관리적 안전성 확보조치를 취하여야 합니다.

개인정보보호법 상담사례집 FAQ

Q7> 내부관리계획을 세워야 한다고 나와 있는데 내부관리계획과 지침을 같은 것으로 보는지, 지침이 있다면 계획은 수립하지 않아도 되나요?

A> 내부관리계획의 수립은 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치 중의 하나입니다(법 제29조). 즉, 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립·시행하는 내부 기준을 의미합니다. 따라서 내부관리계획을 기초로 세부 지침이나 안내서 등을 마련하여 개인정보 취급자 전원이 개인정보 보호에 필요한 동일한 기준에 따라 동일한 행동을 취하도록 할 필요가 있으므로, 내부관리계획은 반드시 수립·시행하여야 하며, 지침과는 별개의 것으로 판단됩니다.

Q8> 개인정보보호법상 '개인정보 처리방침', 정보통신망 이용 촉진 및 정보보호등에 관한 법률상 '개인정보 취급방침'중 어느 것을 사용해야 하나요?

A> 정보통신망 이용촉진 및 정보보호 촉진 및 정보보호 등에 관한 법률의 적용 대상인 정보통신서비스제공자는 개인정보 취급방침을 사용해야 하고, 정보통신망 이용 등에 관한 법률 적용 대상자가 아니라면 개인정보보호법에 따른 개인정보 처리방침을 사용하면 됩니다.

Q9> 내부 직원의 인사정보와 외부 전문가 정보 등의 DB를 관리하고 있습니다. 개인정보보호법에 따라서 별도의 안전장치를 해야 하나요?

A>개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 합니다(개인정보보호법 제29조).

따라서 개인정보를 직접 취급하는 직원 등에 의한 내부자 유출 등을 방지하기 위하여 내부관리계획의 수립·시행, 직원 교육 실시, 전산실·자료보관실 보안구역 설명 및 출입통제, 단말기의 지정·관리 및 접근 권한 제한, 접속기록 보관 및 위·변조 방지 등의 조치를 취해야 합니다.

향후 기업이 대비해야 하는 사항

개인정보 보호법 개정안 2014년 8월 부터 시행!

법률적인 준수 사항 대비

- **2014년 8월 7일 이후로 주민등록번호를 처리하지 않도록 업무체계를 변경**
- **2016년 8월 6일까지 기존 보유하고 있는 주민등록번호의 파기를 이행**
- **예외적으로 보유한 주민등록 번호에 대해 안전성 확보조치를 확실히 수행**

>개인정보 보호법 및 개별법에 따라 개인정보 및 고유 식별 정보에 대한 암호화 필수!!!

>안전성 확보조치 및 관리를 위한 접근권한 관리, 접속기록 관리 필수!!!

기업의 정보 보안 체계 구축

- **기업의 중요한 자산 (고객정보, 및 기밀정보)에 대한 유출 통제 및 차단 방안 체계 구축 필요**
- **외부의 악의적인 침입 및 공격으로부터 고객정보를 보호 방안**
- **고객정보 유출 시 발생할 수 있는 소송 및 피해 최소화 방안**

[참고] 개인정보보호법 요구사항

컴플라이언스 대응:개인정보보호법 > 개인정보의 기술적 관리적 보호조치 방안

통제항목	보호 조치 내역	세부 요건
제8조 접속기록의 위·변조방지	개인정보취급자의 개인정보처리시스템에 대한 접속기록의 위조·변조 방지를 위한 보호조치	①개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하여야 한다. ②개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

[참고] 개인정보보호법 요구사항

컴플라이언스 대응:개인정보보호법

개인정보 보호법 [법률 제10465호, 2011.3.29, 제정]	개인정보 보호법 시행령 [대통령령 제23169호, 2011.9.29, 제정]	개인정보 보호법 시행규칙 [행정안전부령 제241호, 2011.9.29, 제정]
제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.	제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다. 4.개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치	N/A

[참고] 정보통신망법 요구사항

컴플라이언스 대응:정보통신망법

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [법률 제11048호, 2011.9.15, 타법개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 [대통령령 제24102호, 2012.9.14, 타법개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙 [지식경제부령 제92호, 2009.8.28, 타법개정]
제28조(개인정보의 보호조치) ①정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다. 3.접속기록의 위조·변조 방지를 위한 조치	제15조(개인정보의 보호조치) ①법 제28조제1항제1호에 따라 정보통신서비스 제공자등은 개인정보의 안전한 취급을 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다. ③법 제28조제1항제3호에 따라 정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 다음 각 호의 조치를 하여야 한다. 1.개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독 2.개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관	제9조(개인정보의 보호조치) ①법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 관리적 조치는 다음 각 호와 같다. ②법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 기술적 조치는 다음 각 호와 같다. 3.접속기록의 위조·변조 방지를 위한 조치
	제58조(침해사고 관련정보의 제공방법) 법 제48조의2제2항에 따라 침해사고 관련정보를 제공하는 자는 다음 각 호의 방법에 따라 침해사고 관련정보를 제공하여야 한다. 2.침해사고 관련정보의 훼손·멸실 및 변경 등을 방지할 수 있는 조치를 취할 것	

[참고] 금융분야 개인정보보호 법률

소관법령	개인정보 관련내용
금융실명제법	•「금융실명거래법」(97)에 따라 금융거래의 비밀이 보장됨 • 금융실명제법§3에 따라 금융회사등은 거래자의 실지명의로 금융거래를 하여야 함 * 실지명의: 주민등록표에 기재된 성명 및 주민등록번호(개인)
신용정보법	• 금융분야에서의 개인(신용)정보의 수집.이용.제공 등은「신용정보법」(95)에 따라 제한받고 있음 • 특히, 신용정보법§19(시행령§16 및 신용정보감독규정§20)는 개인(신용)정보의 관리와 관련, 신용정보전산시스템에 대한 기술적.물리적.관리적 보안대책을 수립하도록 하고 있어, 개인(신용)정보 오.남용 등을 예방중
전자금융거래법	• 지속적으로 증가하고 있는 전자금융거래에 대해서는「전자금융거래법」(07)에 의해 안전성.신뢰성 확보 의무를 부과하여 건전한 발전을 유도중 • 전자금융거래법§21(전자금융감독규정 제3장§7~§37) 에서는 정보기술부문 및 전자금융업무에 전반에 걸쳐 적용되는 세부적인 안전성 확보조치 사항을 규정

• 위 사항은 **특별법**으로 **개인정보보호법에 우선**하나 **금융거래 고객의 정보에 국한**

•「**개인정보보호법**」**은 일반법**으로 금융거래가 없는 잠재고객의 정보 등 모든 형태의 개인정보가 포함