법무법인 율촌

개인정보 보호법 시행에 따른

보험업계의 대응 전략

2012. 02. 10.

변호사 박재현

Copyright ⓒ 2012 Yulchon, Attorneys at Law. All Rights Reserved.

YULCHON 律村 YULCHON 법무법인 율촌

- 개인정보 보호의 세계적 추세
- 국내 개인정보보호 환경과 문제점
- 개인정보 보호법 제정 및 시행 경과
- 개인정보보호법의 주요 내용
- 가치 선택 이슈 5선
- 개념상 이슈 5선
- 개인정보 보호법의 문제점 7선
- 보험업계의 리스크
- 보험업계의 대응전략

개인정보 보호의 세계적 추세

OECD 가이드라인(1980)

프라이버시보호 및 개인정보의 국제적 유통에 관한 지침

UN 가이드라인(1995)

전산 처리된 개인정보파일의 규제 지침

EU 개인정보 보호지침(1995)

개인정보의 처리 및 자유로운 전송에 관한 개인정보 보호지침

네덜란드 개인정보보호법 제정 및 시행(2001)

일본 개인정보보호법 제정 및 시행(2005)

대한민국 개인정보보호법 제정 및 시행(2011)

*EU 개인정보 보호지침 개정안 발표(2012. 1. 25.): <u>EU 회원국이 아닌 국가에도 적용</u>

국내 개인정보보호 환경과 문제점

세계 최고 수준의 정보화	개인정보 대량 수집·유통 가능성
기업의 개인정보 수집·이용 수요 폭발적 증가	반면 기업의 개인정보 보호에 대한 인식은 상대적으로 낮음
해킹, DDoS, 보이스피싱 등 개인정보 관련 부작용 증가	사전 대응 노력 미흡
정보통신망, 금융·신용정보 등 영역별 개별법률에 의한 보호	개인정보 보호의 사각지대 존재
개인정보 침해 사건은 대형화·지능화·다양화	침해에 따른 Risk도 증가
한·EU FTA, 한·미 FTA	국제적 수준의 정보보호 시스템 구축 필요성

개인정보 보호법 제정 및 시행 경과

17대 국회, 3개 개인정보보호법안 발의

- 노회찬(04. 11), 이은영(05. 7), 이혜훈(05. 12.) 의원안
- 17대 국회 임기만료로 자동 폐기

18대 국회, 3개 개인정보보호법안 발의

- 이혜훈(08. 8), 변재일(08. 10.), 정부안(08. 11.)

국회 본회의 의결(11. 3. 11), 공포(11. 3. 29)

행정안전부 개인정보보호연구회 구성 · 운영(11. 4.)

시행령 및 시행규칙 공포(11. 9. 29), 법 시행(11. 9. 30)

표준지침(11. 10. 4) 및 해설서 발표(11. 12. 15)

계도기간 종료(12. 3. 29)

개인정보 보호법의 주요 내용

영역불문 "개인정보처리자" 에 모두 적용

- 종래에는 영역별로 개별법이 있는 경우에만 적용(약 51만)
- 법 시행으로 공공ㆍ민간 부분의 모든 개인정보처리자에게 적용(약 350만)
- 정보보호에 관한 일반법, 그러나 모든 국민에게 적용되는 것은 아님

임직원, 수탁자 등에 대해서도 적용

전산파일이 아닌 수기문서에도 적용

수집ㆍ이용과 제공ㆍ위탁 및 파기에 관한 새로운 규제

민감정보 및 고유식별정보에 대한 특별한 보호

개인정보보호책임자(CPO)의 지정 의무화

정보주체의 피해구제 강화

- 열람, 정정ㆍ삭제, 처리정지 요구권
- 유출사실 통지신고제
- 집단분쟁조정 및 권리침해중지 단체소송

가치 선택 이슈 5선

무엇을 더 중시해야 하는가?
개인정보의 보호 vs 개인정보 이용의 편의

누구에 대해 어떤 수준의 규제와 권리를 부과할 것인가?
공공기관 vs 민간사업자 vs 개인정보주체

정보의 종류에 따라 규제수준을 달리해야 하는가?
모든 정보를 동일하게 vs 위험성이 큰 정보는 더 중하게

허용 사유를 얼마나 인정할 것인가?
동의 vs 법령상의 근거 vs [편의 또는 필요성이 있는 경우]

정보의 처리 단계별로 규제를 달리할 것인가?
정보의 수집·이용 vs 제공

개념상 이슈 5선

필수적 정보와 선택적 정보의 구별?
마케팅 목적이라고 언제나 선택적 정보는 아닐 수 있음

개인정보의 자기결정권은 일신전속권?
동의권의 대리행사 가능?

14세 이상 20세 미만인 자의 동의 방법?
법정대리인이 취소할 수 있다고 보아야 하는지?

수집 · 이용 · 제공 동의는 묵시적으로도 가능?
원칙적으로 묵시적 동의는 인정 안되나, 명함 · 인터넷 등 예외

삭제 vs 처리정지 vs 파기?
개념상 중첩, 혼동 여지가 있음

개인정보 보호법의 문제점 7선

- 정보 보호에 치중, 이용의 효율성 고려 미흡
- 수집과 제공의 구별 모호
- 제공과 처리위탁을 구별
- 금융업 등 산업특성에 대한 고려가 전혀 없었음
- 동의 받는 절차가 형식적이고 까다로움
- 보유 · 이용 · 파기 기간의 불명확성
- 분쟁조정위원회 결정에 대한 실효성 확보 수단 미흡

보험업계의 리스크

고객정보 관리상의 리스크
기존에 이용하던 정보를 이용할 수 없게 될 리스크

임직원 정보 관리 리스크
근로 관련 분쟁 발생시 약점으로 작용할 수 있음

보험설계사 등 수탁자 관련 리스크
사용자책임 및 평판 리스크/관리상의 어려움

감독 및 제재 관련 리스크
금융감독원, 공정거래위원회 및 행정안전부의 중첩적 규제 가능성

침해사고 및 분쟁 관련 리스크
천문학적 손해배상 책임 부담 가능/ 집단소송 및 분쟁조정제도 도입에 따른 방어비용 증가

보험업계의 대응전략

새로운 규제 체계에 부응하는 시스템 재정비

실무상 필요성을 감안한 세밀한 처리기준 작성, 시행

정보보호 필요성에 대한 인식의 전환

비용과 노력이 수반될 수밖에 없다는 점을 수용하는 자세

치밀한 계약 관리 등을 통한 법적 보호대책 강구

처리위탁 계약 등 각종 서류에 구상권 및 책임제한 등 조치 필요

관련 법령상 요구되는 절차는 반드시 준수

제재 및 사용자 책임 등을 면하기 위하여 필수적으로 필요

새로운 보험상품의 개발

기업의 전문학적 손해배상 책임에 대비한 보험상품 등 개발/
침해사고에 따른 손해산정 등에 대한 노하우 축적

감사합니다

박재현 변호사

Tel: +82-2-528-5636

E-mail: jpark@yulchon.com

YULCHON 律村 법무법인 율촌

서울 특별시 강남구 대치 2동 944-31 섬유센터 12층

Tel: 02-528-5200

Fax: 02-528-5228

E-mail: mail@yulchon.com

보험사업 영위와 관련된 개인정보보호 이슈

김재영 변호사

bkl 법무법인(유)태평양

Overview

- 보험사업의 진행 단계에 따른 개인정보 보호 이슈
- 현행 개인정보 보호법의 문제점 및 개선방향
- 개인정보 보호 관련 최근 이슈

1 보험사업의 진행단계에 따른 개인정보 보호 이슈

- 보험모집 단계에서의 개인정보 수집
- 개인정보의 관리
- 개인정보를 활용한 보험상품 마케팅
- 수집한 개인정보의 파기
- 기타 관련 이슈

보험사업의 진행단계에 따른 개인정보 보호 이슈

보험 모집 단계에서의 개인정보 수집

보험회사는 정보주체인 보험계약자 등에게 일정한 사항을 고지하고 그 동의를 받아 개인정보를 수집하고, 고지된 목적 범위 내에서 개인정보를 이용하여야 함.

동의 예외 사유 (개인정보 보호법 제15조 제1항)

- **법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우** (예컨대 보험회사가 상법 제719조에 따른 보상책임의무를 이행하기 위하여 불가피한 경우 피해자의 동의 없이 피해자의 개인정보를 수집·이용할 수 있음)
- **청약자와 보험계약 체결 및 이행을 위하여 불가피하게 필요한 경우**: 개인정보를 수집, 이용하지 않고는 청약자와 계약을 체결하고, 체결된 계약의 내용에 따른 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우에는 동의 없이 개인정보 수집 가능. 예컨대, 보험회사가 계약체결을 위해 청약자의 자동차사고이력, 다른 유사 보험의 가입 여부 등에 관한 정보를 수집하는 경우에는 청약자의 동의 불필요. 단, 보험계약 미체결시에는 수집한 개인정보는 즉시 파기하여야 함.
- 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 **사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우**
- 개인정보처리자의 **정당한 이익을 달성하기 위하여 필요한 경우**로서 명백하게 정보주체의 권리보다 우선하는 경우(이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한함)

보험사업의 진행단계에 따른 개인정보 보호 이슈

보험가입설계서 발행과 개인정보 수집

- 보험계약 체결 권유 단계에게 고객이 직접 개인정보(주민등록번호 제외)를 보험모집인에게 제공하면서 보험가입설계서 발행에 구두로 동의한 경우 보험회사 또는 보험모집인이 고객의 별도 동의 없이 개인정보를 수집하여 이용할 수 있는지가 문제됨
- 행정안전부는 "정보주체와의 계약의 체결 및 이행을 위하여 불가피한 경우에 해당한다고 볼 수 있으므로 보험계약의 목적 범위 내에서는 별도의 동의 없이 개인정보(민감정보 및 고유식별정보 제외)를 수집 · 이용할 수 있"다고 유권해석(2011. 12. 11. 개인정보보호과-4375).

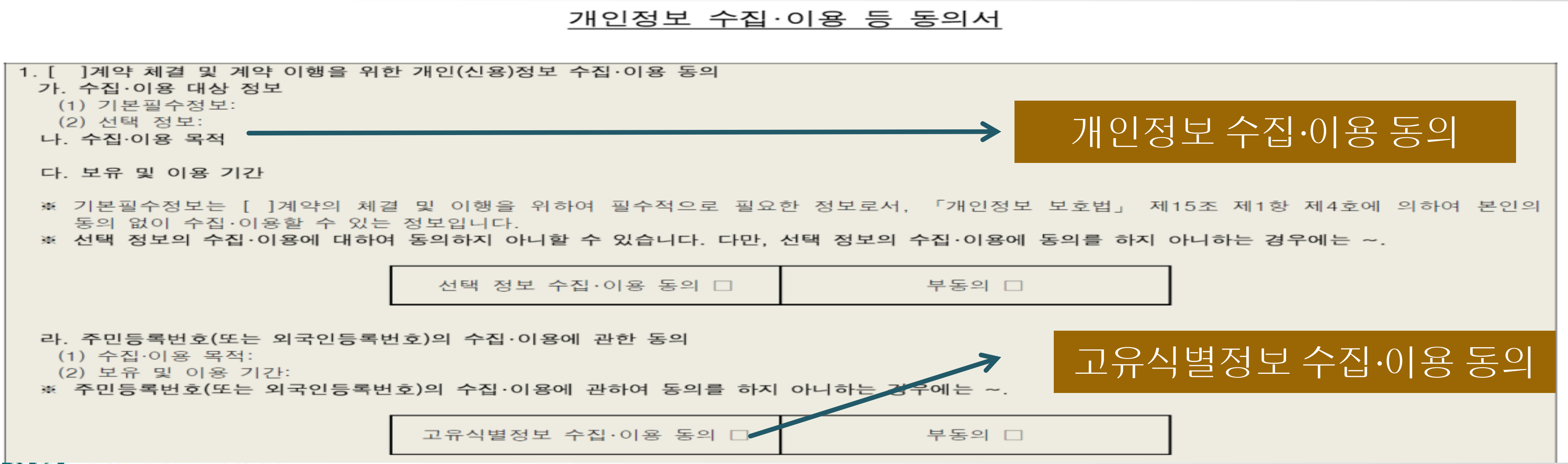
청약자로부터 명함을 받은 경우

- 청약자가 자신의 명함을 보험회사의 직원, 보험설계사 등에게 교부하는 행위에는 명함에 기재된 정보를 사용해도 좋다는 동의가 내재되어 있다고 해석(행정안전부). 그러므로 명함에 기재된 청약자의 개인정보를 이용하기 위해 청약자의 동의를 받을 필요 없음.
- 단, 청약자가 명함을 교부한 목적(예컨대, 보험계약 체결) 이외의 다른 목적(마케팅 등)을 위해 명함에 기재된 정보를 사용하거나 그 개인정보를 제3자에게 제공하기 위해서는 청약자의 동의 필요.

보험사업의 진행단계에 따른 개인정보 보호 이슈

보험설계사 또는 보험대리점이 보험계약자의 개인정보를 수집하는 경우의 업무위탁 관계

- 보험회사와 위촉계약을 체결한 보험설계사 또는 보험대리점이 보험을 모집하면서 보험계약자 등으로부터 개인정보 수집 동의를 받는 것은 보험회사의 개인정보 처리업무를 위탁 받아 처리하는 것으로 볼 수 있음.
- 보험회사는 보험설계사 또는 보험대리점에게 개인정보 수집 업무를 위탁함에 있어 ① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항, 위탁업무의 목적 및 범위 등의 내용이 포함된 문서에 의하여야 하며, ② 위탁업무의 내용과 수탁자에 관한 사항을 보험회사의 인터넷 홈페이지에 지속적으로 게재하는 방법으로 공개하여야 함(개인정보 보호법 제26조; 게재 범위에 대해서는 뒤에서 살펴봄).


개인정보 수집·이용 등 동의서

1. [ ]계약 체결 및 계약 이행을 위한 개인(신용)정보 수집·이용 동의
가. 수집·이용 대상 정보
(1) 기본필수정보:
(2) 선택 정보:
나. 수집·이용 목적

다. 보유 및 이용 기간

※ 기본필수정보는 [ ]계약의 체결 및 이행을 위하여 필수적으로 필요한 정보로서, 「개인정보 보호법」 제15조 제1항 제4호에 의하여 본인의 동의 없이 수집·이용할 수 있는 정보입니다.
※ 선택 정보의 수집·이용에 대하여 동의하지 아니할 수 있습니다. 다만, 선택 정보의 수집·이용에 동의를 하지 아니하는 경우에는 ~.

선택 정보 수집·이용 동의 □	부동의 □

라. 주민등록번호(또는 외국인등록번호)의 수집·이용에 관한 동의
(1) 수집·이용 목적:
(2) 보유 및 이용 기간:
※ 주민등록번호(또는 외국인등록번호)의 수집·이용에 관하여 동의를 하지 아니하는 경우에는 ~.

고유식별정보 수집·이용 동의 □	부동의 □

보험사업의 진행단계에 따른 개인정보 보호 이슈

청약자의 동의 없이 수집할 수 있는 개인정보의 범위

- 청약자의 동의 없이 수집할 수 있는 개인정보는 계약의 체결 및 이행을 위해 필수적인 정보, 법령상 의무준수를 위해 불가피한 정보, 급박한 생명 · 신체 · 재산상 이익보호를 위해 필요한 정보 등이 있음(개인정보 보호법 제15조).
- 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 정보만 수집하여야 함(최소수집의 원칙).
- 개인정보를 수집하는 보험회사가 필요한 최소한의 정보에 해당하는지 여부를 입증하여야 함
  → 필수정보의 범위를 최소화할 필요.

최소한 정보 이외의 개인정보 수집에 동의하지 않을 경우 보험계약 체결 거부 가능?

- 청약자가 보험계약 체결 등을 위해 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않았다는 이유로 보험계약의 체결이나 기타 서비스의 제공을 거부할 수 없음(개인정보 보호법 제16조 제2항).
- 필수정보 이외의 정보 수집에 동의하지 않는다는 이유로 서비스 제공 등을 거부하면 3천만 원 이하의 과태료 부과.

보험사업의 진행단계에 따른 개인정보 보호 이슈

단체보험계약 및 퇴직연금계약 체결에 따른 개인정보 수집 동의의 문제

- 기업의 단체보험계약 및 퇴직연금계약을 체결할 때 기업 직원들의 개인정보를 수집함에 있어서는 개별 직원들로부터 개별적으로 동의를 받아야 하는지가 문제.
- 현행 개인정보 보호법 상으로는 단체보험계약 및 퇴직연금계약 시 개인정보 수집 동의의 범위를 다른 계약과 달리 볼 근거가 없으므로, <u>기업 직원들로부터 개별 동의를 받아야 할 것</u>으로 보임. 다만, 상법 제735조의 3 제1항, 제739조에 의하면 <u>기업의 규약(단체협약, 취업규칙, 정관)에서 단체보험에 관한 규정을 둔 경우에는 별도로 개별 직원의 동의 불요</u> (행정안전부).
- 퇴직연금의 경우에도 단체보험과 마찬가지로 기업 규약에서 퇴직연금에 관한 규정을 두었다면 별도로 개별 직원의 동의가 필요한지 여부에 대하여 판단한 선례나 견해가 없어 논란의 여지가 있음

보험사업의 진행단계에 따른 개인정보 보호 이슈

보험계약자가 대리인을 통해 계약을 체결할 경우

- 보험계약자가 대리인을 통해 보험계약을 체결할 경우, 그 대리인이 정당한 대리권을 부여 받았는지 여부에 관한 정보는 계약체결을 위해 반드시 필요한 정보로서, 대리인 여부를 확인하기 위하여 대리인의 개인정보를 수집 및 이용할 수 있음. 예컨대, 보험계약자와 대리인의 관계를 알 수 있는 정보, 대리권 부여에 관한 보험계약자의 의사를 확인하기 위하여 보험계약자의 연락처에 관한 정보 등은 동의 없이 수집 가능. 단, 대리인의 주민등록번호 등 고유식별정보를 수집할 때에는 동의 필요.

미성년자의 개인정보를 수집할 경우

- 만 14세 미만 아동의 개인정보를 수집하기 위하여 동의를 받아야 할 필요가 있을 경우에는 그 법정대리인의 동의 필요 (개인정보 보호법 제22조 제5항).
- 만 14세 초과 미성년자의 개인정보를 수집하기 위하여 동의를 받아야 할 경우에는 법정대리인이 아닌 해당 미성년자의 동의로도 가능

개인정보의 관리

안전성 확보 조치 의무 (개인정보 보호법 제29조)

- 수집한 개인정보의 안전한 처리를 위한 내부 관리계획을 수립하고 시행
- 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치, 개인정보를 안전 용 또는 이에 상응하는 조치, 개인정보 침해사고의 발생에 대응하기 위 조치, 개인정보에 대한 보안프로그램의 설치 및 갱신 등 기술적 보호조
- 개인정보의 안전한 보관을 위한 보관시설의 마련, 잠금장치의 설치 등

개인정보 처리방침의 수립 및 공개 (개인정보 보호법 제30조)

- 개인정보의 처리 목적, 개인정보의 처리 및 보유기간, 개인정보의 제3자 한 사항 등이 포함된 개인정보 처리방침을 수립하고, 그 방침을 인터넷 홈페이지에 지속적으로 게재하여야 함.

개인정보 내부관리계획 목차 (예시)

제1장 총칙
제1조(목적)
제2조(적용범위)
제3조(용어 정의)

제2장 내부관리계획의 수립 및 시행
제4조(내부관리계획의 수립 및 승인)
제5조(내부관리계획의 공표)

제3장 개인정보보호책임자의 의무와 책임
제6조(개인정보보호책임자의 지정)
제7조(개인정보보호책임자의 의무와 책임)
제8조(개인정보취급자의 범위 및 의무와 책임)

제4장 개인정보의 처리단계별 기술적·관리적 안전조치
제9조(개인정보취급자 접근 권한 관리 및 인증)
제10조(접근통제)
제11조(개인정보의 암호화)
제12조(접근기록의 위변조 방지)
제13조(보안프로그램의 설치 및 운영)
제14조(물리적 접근제한)

제5장 개인정보보호 교육

제6장 개인정보 침해대응 및 피해구제

보험사업의 진행단계에 따른 개인정보 보호 이슈

개인정보 보호책임자 지정 (개인정보 보호법 제31조)

- 보험회사는 사업주 또는 대표자, 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람을 개인정보 처리에 관한 업무를 총괄하고 책임질 개인정보 보호책임자로 지정하여야 함.
- 개인정보 보호책임자는 개인정보 보호 계획의 수립 및 시행, 개인정보 처리 실태 조사 및 개선, 개인정보 처리와 관련한 불만의 처리 및 피해 구제, 내부통제시스템 구축, 교육 계획 수립 및 시행, 개인정보파일 보호 및 관리 · 감독 등의 업무를 수행.
- 정보통신망법에 따른 개인정보보호책임자, 신용정보법에 따른 신용정보보호책임자와 겸임 가능

정보주체의 개인정보 열람 등 권리 보장 (개인정보 보호법 제35조, 제36조, 제37조)

- 보험회사는 정보주체가 개인정보 열람 · 정정 · 삭제 · 처리정지를 요청할 수 있는 구체적 방법과 절차를 마련하고, 정보주체가 알 수 있도록 공개하여야 함.

BAE, KIM & LEE LLC

보험사업의 진행단계에 따른 개인정보 보호 이슈

개인정보를 이용한 보험상품 마케팅

보험회사가 수집한 개인정보를 활용한 보험상품 마케팅

- 보험회사가 수집한 보험계약자, 피보험자 등의 개인정보를 활용하여 자사의 보험상품을 마케팅하기 위해서는 해당 정보주체에게 마케팅 목적으로 정보를 수집한다는 사실을 명확하게 알리고 다른 동의와 구분하여 동의를 받아야 함(개인정보 보호법 제22조 제2항).
- 보험계약 체결을 목적으로 수집한 개인정보를 사전 동의 없이 자사의 별도 보험상품이나 서비스를 마케팅하는데 이용해서는 안 됨.
- 보험계약자의 보험가입정보나 보험료 납부현황 등의 신용정보는 보험계약자의 동의가 없는 한 보험계약의 설정 및 유지 여부를 판단하기 위한 목적으로만 이용하여야 함(신용정보의 이용 및 보호에 관한 법률 제33조).

학교 졸업앨범, 동창회 명부 등 공개된 정보를 이용한 보험상품 마케팅

- 학교의 졸업앨범, 동창회 명부, 인터넷 홈페이지 등에 공개된 정보는 그 공개된 목적의 범위에서만 이용가능. 예컨대, 졸업앨범의 경우 동문들의 상호 연락 및 친목 도모 등 목적으로만 이용 가능.
- 공개된 정보라 하더라도 그 정보주체로부터 별도로 동의를 받지 않는 이상 보험상품 마케팅에 이용할 수 없음

보험사업의 진행단계에 따른 개인정보 보호 이슈

보험회사 수집 개인정보를 활용한 보험설계사의 보험상품 마케팅

- 보험회사의 보험설계사에 대한 개인정보 제공은 개인정보 처리 업무의 위탁으로 볼 가능성이 높음.
- 보험회사가 보험설계사에게 개인정보의 처리를 위탁하는 경우에는 ① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항, 위탁업무의 목적 및 범위 등의 내용이 포함된 문서에 의하여야 하며, ② 위탁업무의 내용과 수탁자에 관한 사항을 보험회사의 인터넷 홈페이지에 지속적으로 게재하는 방법으로 공개하여야 함.
- 보험회사가 보험상품의 마케팅 업무를 보험설계사에게 위탁하는 경우에는 그 위탁하는 업무의 내용과 수탁자를 정보주체에게 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법으로 고지하여야 함. 보험회사가 과실 없이 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 함(개인정보 보호법 제26조, 같은 법 시행령 제28조).
- 보험회사와 위촉계약을 체결한 전체 보험설계사의 명단을 인터넷 홈페이지에 게재하거나 정보주체에게 알려야 하는지에 대하여는 논란이 있음. 카테고리별 고지만으로 가능한지 여부에 대하여 행정안전부 등 감독관청의 입장이 명확하게 정해지지 않았으므로 최대한 안전하게 접근할 필요가 있음.
- 보험회사가 보험계약자의 보험가입정보, 보험료 납부현황 등 신용정보를 보험설계사에게 제공할 경우에는 정보주체의 사전동의 필요(신용정보의 이용 및 보호에 관한 법률 제32조 제1항, 같은 법 시행령 제28조 제1항, 제2조 제2항).

보험사업의 진행단계에 따른 개인정보 보호 이슈

텔레마케터를 활용한 보험상품 마케팅 과정에서 보험회사가 수집한 개인정보 활용 가능?

- 텔레마케터가 보험회사와 고용관계에 있는 근로자인지 보험설계사로서 위촉계약을 체결한 제3자인지 불분명.
- 하급심은 텔레마케터는 일반적인 보험모집인과 달리 근로자에 해당한다고 판시(서울행정법원 2006. 4. 19. 선고 2005구합32873 판결, 서울행정법원 2008. 3. 21. 선고 2007구합19539 판결).
- 하급심의 취지대로라면 텔레마케터가 보험회사에 의하여 적법하게 수집된 개인정보를 활용하여 보험상품을 마케팅하는 경우, 별도로 정보주체로부터 동의를 받거나 업무 위탁을 고지하지 않더라도 개인정보 보호법 위반이 아니라고 판단될 가능성이 있음. 다만, 사전에 개인정보 수집 시에 마케팅을 위하여 개인정보를 수집한다는 사실을 정보주체에게 알리고 동의를 받을 필요가 있음.
- 보험회사와 보험계약을 체결한 실적이 있는 보험계약자와 현재 유효한 보험계약의 피보험자에 대하여는 사전 동의가 없더라도 통신수단을 이용한 마케팅이 일응 가능할 것으로 보임(보험업법 제96조 제1항, 시행령 제43조 제1항 제2호).
- 텔레마케터에게 개인정보 내용을 밝히지 않고 자동 다이얼링시스템을 이용하여 보험상품 마케팅을 하도록 하는 경우에는 개인정보 보호법 위반 문제가 발생할 가능성이 낮아질 것으로 보임.

수집한 개인정보의 파기

- 개인정보의 보유기간 경과, 보험기간 만료 등 개인정보 처리 목적 달성으로 인하여 그 개인정보가 불필요하게 되었을 때에는 그 사유가 발생한 날로부터 5일 이내에 복구 또는 재생되지 아니하는 방법으로 개인정보를 파기하여야 함(개인정보 보호법 제21조).
- ‘복구 또는 재생되지 아니하는 방법’은 사회통념상 현재 기술 수준에서 적절한 비용이 소요되는 방법을 의미.
- 다른 법령에 따라 개인정보를 보존하여야 하는 경우에는 개인정보를 파기하지 않아도 무방. 예컨대, 전자금융거래법에 의하면 금융기관은 전자금융거래에 관한 기록을 그 종류에 따라 5년 또는 1년간 보존하여야 함.

기타

보험설계사 모집정보의 집적 및 활용

- 보험설계사의 잦은 회사 이동 변경으로 인한 보험계약 조기실효, 미환수 수수료 급증 등 모집질서 혼탁 및 소비자 피해를 방지하기 위하여 보험회사가 보험설계사의 모집정보를 집적 및 활용하는 경우가 있음.
- 보험회사는 보험설계사로부터 일정한 모집정보(개인식별정보 및 총 계약건수 중 품질보증해지 건수, 수당환수 내역 유무, 보증보험 가입 및 청구여부)를 수집하기 위하여 해당 보험설계사로부터 '모집정보 수집 · 이용'에 대한 동의를 받아야 함.
- 만약 모집정보에 보험계약자의 개인정보가 포함되어 있다면 그 보험계약자의 동의까지 받아야 함.
- 위와 같이 수집한 모집정보를 생명보험협회 내지 손해보험협회에 제공하고 그 각 협회가 여러 보험회사에 제공할 수 있도록 하기 위해서는 그러한 목적을 특정하여 동의를 받아야 함.

보험사업의 진행단계에 따른 개인정보 보호 이슈

책임보험에서 정한 보험사고 발생시 피해자의 개인정보 수집

- 책임보험계약의 보험자는 피보험자가 보험기간 중의 사고로 인하여 제3자에게 배상할 책임을 지는 경우 보상책임의무 발생(상법 제719조).
- 보험회사는 위 보상책임의무를 이행하기 위하여 불가피한 경우에는 피해자의 동의 없이 피해자의 개인정보를 수집하여 이용할 수 있음(법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우).

보험계약자나 피보험자 등의 개인정보를 범죄 수사 목적으로 수사기관에 제공 가능?

- 공공기관이 아닌 보험회사는 비록 범죄 수사 목적이라 하더라도 형사소송법 등 법령에서 정한 절차에 따라서만 보험계약자나 피보험자 등의 개인정보를 수사기관에 제공할 수 있고, 그 이외 임의 제공은 불가능.

보험사업의 진행단계에 따른 개인정보 보호 이슈

보험계약자 또는 피보험자 등의 개인정보를 재보험자에게 제공 가능?

- 보험회사가 재보험자와 재보험계약을 체결하거나(임의재보험) 또는 원보험계약 체결시마다 재보험에 부보되는 경우(자동재보험) 보험계약자 또는 피보험자 등의 개인정보를 재보험자에게 제공하기 위해서는 해당 정보주체의 제3자 제공에 대한 동의 필요.

2 현행 개인정보 보호법의 문제점 및 개선방향

- 현행 개인정보 보호법의 문제점
  - 법률적용의 중첩
  - 소관부서의 중첩 가능성
  - 모순되는 법률규정의 존재
  - 고유식별정보의 수집 제한
  - 단체보험 및 퇴직연금 영업상의 비효율성
- 법개정의 움직임

현행 개인정보 보호법의 문제점

법률적용의 중첩

- 보험회사에 적용되는 개인정보 보호법제로 신용정보법, 정보통신망법 등에 더하여 개인정보 보호법이 추가됨.
- 보험회사의 영업형태에 따라 그에 상응하는 개인정보 보호법제가 중첩적으로 적용되고, 개인정보 보호법의 제정으로 그 중첩성이 더욱 심화됨.
- 그런데 개인정보 보호법 제6조는 그 적용범위를 다소 모호하게 규정하고 있음("개인정보 보호에 관하여는 정보통신망법, 신용정보법 등 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법이 정하는 바에 따른다.").
- 특히, 통신판매의 경우 보험업감독규정 제4-36조 제2항에서는 "통신판매에 관한 업무를 영위하는 자는 개인정보의 수집 · 활용 · 제공에 있어 관계법령을 준수"하여야 한다고 규정하고 있을 뿐, 관계법령이 무엇인지, 어느 정도까지 준수해야 하는지에 대해서는 전혀 내용이 없음.
- 이와 같이 개인정보 보호법제는 중첩적으로 적용되는 반면, 법률의 적용범위는 불분명한 점이 있음.

현행 개인정보 보호법의 문제점 및 개선방향

소관부서의 중첩 가능성

- 한 사업자에 대하여 개인정보 보호법과 정보통신망법이 중첩적으로 적용될 수 있음.
- 그런데 각 법률의 소관부서가 달라서(정보통신망법은 방송통신위원회, 개인정보 보호법은 행정안전부), 해당 법률 집행시 규제의 중첩이 발생할 우려가 있음.
  - 예: 개인정보 보호법 제34조에서는 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에 지체 없이 해당 정보주체에게 관련 사실들을 통보해야 한다고 규정한 반면, 이에 대하여 정보통신망법(2011. 12. 29.자 국회통과 이전의 법)은 아무런 규정을 두고 있지 않음. 따라서 정보주체에 대한 통보문제가 포함된 개인정보 유출사고가 발생한 경우, 원칙적으로 방송통신위원회가 사고조사를 수행하게 되지만, 통보문제에 대해서는 행정안전부가 재차 개입할 가능성이 있음.
- 이에 대하여 개인정보보호위원회, 행정안전부, 방송통신위원회를 비롯하여 각 관련 부처에서 협의를 통하여 해결 방안을 모색 중에 있음

현행 개인정보 보호법의 문제점 및 개선방향

모순되는 법률규정의 존재

- 예 1 – 고유식별정보의 처리
  - 개인정보 보호법은 원칙적으로 주민등록번호 등의 고유식별정보의 처리를 금지하면서, 정보주체의 별도 동의 및 법령의 근거가 있는 등의 경우에만 예외적으로 허용하고 있음(제24조).
  - 그러나 정보통신망법 및 공직선거법 등에서는 여전히 주민등록번호 등(i-Pin 등과 같은 고유식별번호 포함)의 활용을 전제로 인터넷 실명제를 규정하고 있음(다만, 2011. 12. 29. 통과된 개정 정보통신망법은 주민등록번호의 원칙적 사용 제한 규정을 두고 있음).
  - 그리고 전자상거래 등에서의 소비자보호에 관한 법률은 거래기록 보존의 목적에서, 게임산업진흥에 관한 법률은 청소년 보호의 목적(소위 셧다운제)에서, 주민등록번호를 활용한 인증 및 보존을 규정하고 있음.
- 예 2 – 수집 저장하고 있는 정보의 암호화 범위
  - 개인정보 보호법 : 비밀번호와 바이오 정보 / 고유식별정보는 위험도 분석에 따라 암호화 의무가 달라짐
  - 정보통신망법 : 비밀번호, 바이오 정보, 주민등록번호, 신용카드번호, 계좌번호
  - 신용정보법 : 패스워드, 생체정보 등 본인임을 인정하는 정보
- 개인정보 보호법의 원칙과 모순되는 규정들이 여전히 다른 법률에 존재하고 있음.

현행 개인정보 보호법의 문제점 및 개선방향

고유식별정보의 수집 제한의 원칙

- 개인정보 보호법은 고유식별정보에 대하여 원칙적으로 수집을 금지하고, 정보주체로부터 동의를 받거나 법령상의 예외가 있는 경우에만 고유식별정보의 수집을 허용하고 있음.
- 그런데 할인할증률 적용, 중복계약 확인 및 보험금 지급업무 등의 수행을 위하여 고유식별정보는 보험회사에 반드시 필요한 정보임.
- 따라서 고유식별정보의 수집 제한의 원칙이 강조될 경우 보험사업의 운영에 차질이 야기될 우려가 있음.

현행 개인정보 보호법의 문제점 및 개선방향

단체보험 및 퇴직연금 영업상의 비효율성

- 개인정보 보호법에 따르면, 보험회사는 주민등록번호, 이름 등 개인정보를 확인 및 수집하기 위해서는 이용목적과 보유 및 이용기간까지 포함하여 반드시 당사자의 서면 동의를 받아야 함.
- 앞서 본 것처럼 단체보험과 퇴직연금에 대해서도 상법 상의 예외 이외에는 별다른 예외조항이 없어 보험회사는 해당 기업 전체 직원들의 개별 서면동의를 받아야 하는 것으로 해석됨.
- 그러나 해당 기업 직원들 모두로부터 서면 동의서를 일일이 받는다는 것은 사실상 불가능하고 이를 위하여 추가되는 사업비도 상당할 것으로 예상되는 등 보험영업상 비효율을 초래할 우려가 매우 큼.

현행 개인정보 보호법의 문제점 및 개선방향

법개정의 추진

•보험업계에서는 보험업법 시행령을 개정하여 단체보험 취급시, 보험수익자 동의시, 타인을 위한 보험계약 체결시, 제3자 배상시 등의 경우 개인정보 수집 등의 예외를 인정하여 줄 것을 행정안전부에 지속적으로 요청하여 왔음.

•이에 따라 위와 같은 내용을 상당 부분 반영한 보험업법 시행령 개정안이 2011. 9. 9.자로 입법예고되었으나 법제사법위원회에서 최종 통과되지 않음.

- 현재 보험업계의 의견을 수집하면서 보험업법 시행령 개정을 위한 재작업이 진행중인 것으로 알려져 있음.
- 금융위원회에서는 별도의 지침을 제정하지 않고 가망고객 동의 예외 인정(1개월간) 등을 "금융위원회 참고사항 안내"를 통해 해소할 예정이었음. 그러나, 보험업법 시행령의 개정이 늦어짐에 따라 현재는 작업이 중단된 상태라고 함.

3 개인정보 보호 관련 최근 이슈

- 개인정보의 국외이전 문제
- 개인정보 보호법과 타법간의 정합성 문제
- 규제강화 움직임

개인정보의 국외 이전 문제

배경

- 글로벌 보험회사의 경우 개인정보가 포함된 보험 관련 정보를 외국에 있는 본사에서 통합하여 관리하는 경우가 있음
- 이 경우 개인정보의 국외 이전 문제가 발생하고 관련 법령상 요건을 구비하여야 함
- 최근 개인정보 보호법의 시행에 따라 글로벌 보험회사들이 특히 자문을 많이 구하는 이슈임

관련 규정

- 개인정보 보호법 제17조 제3항: 개인정보를 국외의 제3자에게 제공하는 경우 정보주체의 동의를 받아야 함
- 정보통신망법 제63조: 이용자의 개인정보를 국외로 이전하는 경우 이용자의 동의를 받아야 함
- 인터넷을 통하여 보험서비스를 제공하거나 개인정보를 처리하는 보험회사의 경우에는 정보통신망법도 적용됨
- 개인정보 보호법과 정보통신망법 규정의 문언상 차이로 인해 적용범위에 차이가 있음

개인정보 보호법과 타법간의 정합성 문제

배경

- 개인정보 보호법은 정보통신망법, 신용정보보호법 등 개인정보 보호에 관한 개별법이 이미 마련된 이후에 제정되어 일반법과 특별법, 신법과 구법간의 관계 설정이 다소 미흡하고 해석상 논란의 여지가 많음
- 예를 들어 온.오프라인 겸업 사업자는 정보통신망법과 개인정보보호법 모두가 적용이 가능함에 따라 법 적용에 대한 혼란 발생 가능성 존재

동향

- 개인정보보호위원회 등 관련 기관에서 관련 문제점을 인식하고 정비작업을 추진하고 있음
- 현재 관련 전문가들로부터 의견을 수집하고 있으며 아직 내부적으로도 입장이 정리되지 않았음
- 다양한 국내외 기업들이 개인정보 보호법의 해석 및 적용과 관련된 관련 기관의 입장을 문의하고 있는 상황이나 아직 명확한 답변을 주지 못하고 있는 것이 현실임
- 향후 관련 기관의 입장에 주목할 필요가 있음

개인정보 보호 관련 최근 이슈

규제강화 움직임

배경

- 개인정보 보호법 시행 초기 행정안전부는 6개월 간의 유예기간을 두고 계도하겠다는 입장을 밝힌 바 있음
- 최근 사회적으로 이슈가 되는 개인정보 침해사고가 발생하였음
- 기존의 개인정보 보호 관련 일반법 역할을 한 정보통신망법의 주관기관인 방송통신위원회와 개인정보 보호법의 주관기관인 행정안정부, 최근 금융 사고의 발생으로 인한 금융위원회 등 관련 기관들의 경쟁적 움직임
- 강화된 EU 가이드라인의 시행이 예정되어 있고, 이는 국내 법의 추가 보호조치를 규정하게 하는 계기가 될 가능성이 있음

동향 및 대응방안

- 유예기간의 경과 후 행정안정부의 법집행 의지 – 개인정보 보호법의 실효성 확보, 개인정보 보호 관련 규제기관으로서의 위상 제고
- 개인정보 침해사고에 따른 규제 강화 움직임(예, 현재 노출 또는 유출된 주민등록번호를 즉시 삭제하도록 권고하고 있는데 이를 법적 의무로 부과하는 방안에 대해 검토 중)

감사합니다

jyk@bkl.co.kr
www.bkl.co.kr

bkl 법무법인(유)태평양

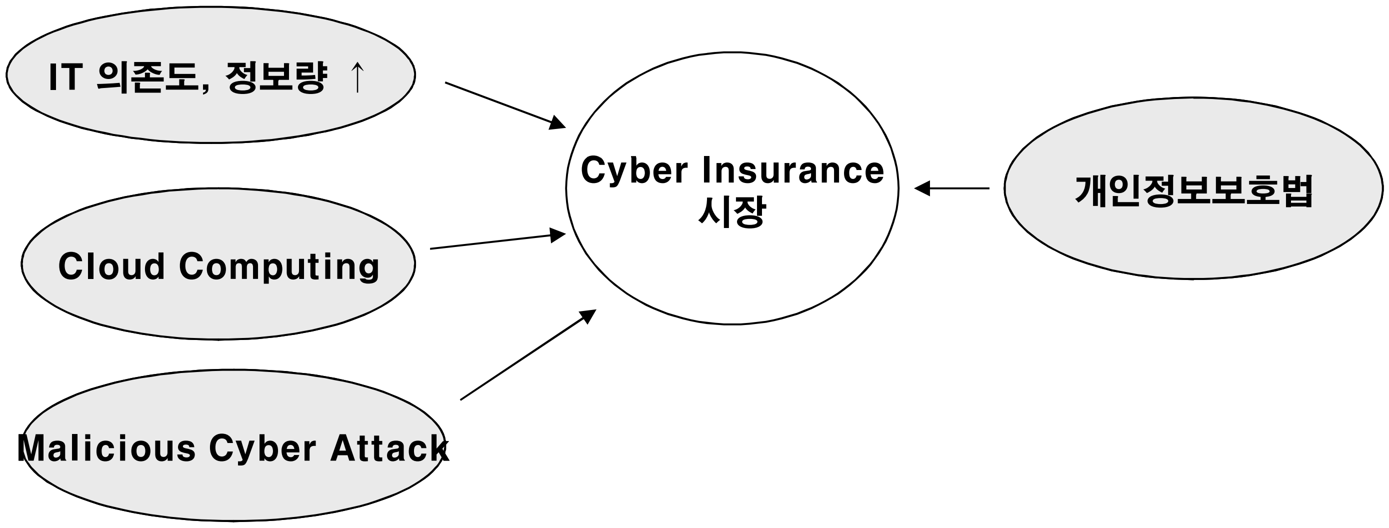
개인정보 관련 리스크관리와 보험산업

2012. 2. 10

변혜원

보험연구원

Motivation

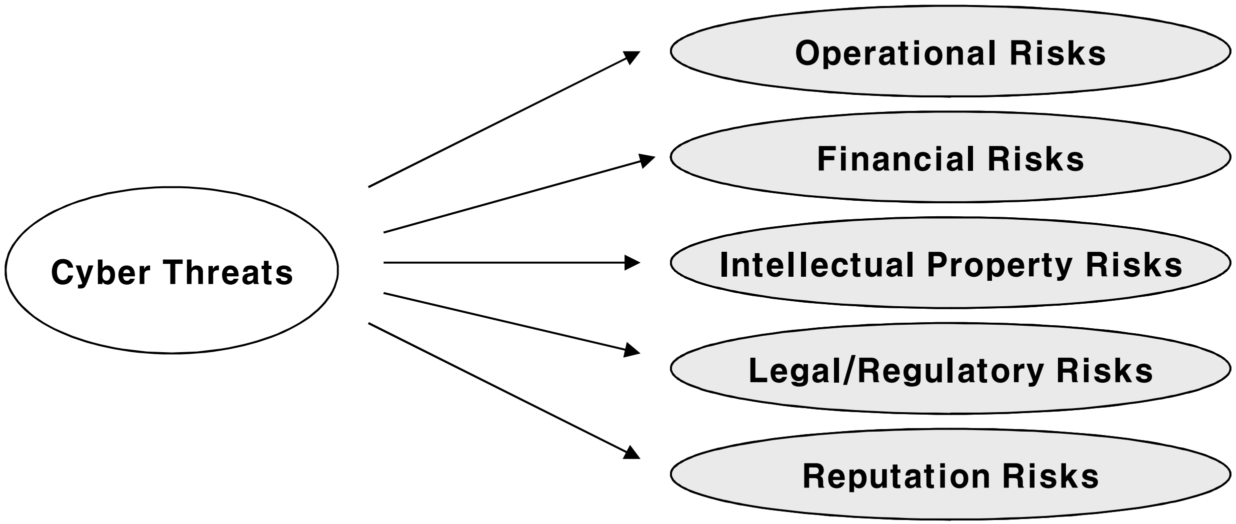

IT 의존도, 정보량 ↑
Cloud Computing
Malicious Cyber Attack
Cyber Insurance
시장
개인정보보호법

Road Map

- Cyber Risk
- 개인정보 유출 현황
- 개인정보보호 관련 제도: 국내 및 해외
- 해외 Cyber 보험시장
- 국내 Cyber 보험시장
- 맺음말

Cyber Risk

❖ Cyber Risk 는 전자상거래 또는 정보기술을 매개로 하여 이루어지는 활동(일반영업이나 운영)에서 발생할 수 있는 위험을 포괄



자료: Lloyds (2010)

Cyber Risk

	손실	손실 객체	손인
당사자 리스크	재산손해	S/W(프로그램), 데이터	해킹, 바이러스, 프로그램오류
	도난,사기	데이터, S/W, 지적재산권	종업원, 외부인
	간접손해	휴업에 따른 수익상실	해킹, 바이러스, 범죄악용, 시스템 고장
	재화손실 (extortion)	돈의 교환에 따른 손실, 금전적으로 회사를 궁핍하게 함	범죄로 이용되고 있는 컴퓨터로부터 얻은 정보나 접근 허용
제 3 자 리스크	법률배상 책임	일반적 손해	접근의 제한, 도난컴퓨터로부터 제3자정보 보호에 불충분한 장치사용, 바이러스 확산
		지적재산권 침해	저작권/상표권 노출, 거래비밀 (R&D, 업무절차, 고객목록),
		콘텐츠, 광고 손해	명예실추, 프라이버시 침해, 민감정보의 불법적인 유통

자료: 보험연구원 용역보고서 (2011)

개인정보 유출 현황: 국내

❖ 금융기관 개인정보 유출 현황

- 현대캐피탈 해킹 사건 (2011. 4): 132만 여명의 개인정보 유출
- 농협 전산망 장애 (2011.4): 사건 기간 동안 수수료 면제, 카드대금 결제 연기 등에 따른 피해액 100억 원
- 리딩투자증권 서버, 한국전자금융 홈페이지 해킹 (2011. 5)
- 삼성카드 (2011. 8): 고객 개인정보 80만 건 유출
- 하나SK카드 (2011.9): 고객 개인정보 10만 건 유출

개인정보 유출 현황: 국내

- 금융회사 이외에도 SK Communications와 Nexon의 개인정보 유출사건은 규모가 큰 사건

<전세계 개인정보 DB 유출 사건 및 기록 현황>

순위	건수	날짜	회사명
1	130,000,000	2009. 1.20	Heartland Payment Systems(미국)
2	94,000,000	2007. 1.17	TJX Companies Inc.(미국)
3	90,000,000	1984. 6.01	TRW, Sears Roebuck(미국)
4	77,000,000	2011.4.26	Sony Corporation(미국)
5	40,000,000	2005. 6.19	Card Systems, Visa, Mastercard, American Express(미국)
6	40,000,000	2011.12.26	Tianya(중국)
7	35,000,000	2011.7.28	SK Communications, Nate, Cyworld(한국)
8	35,000,000	2011.11.10	Steam (Valve, Inc.) (미국)
9	32,000,000	2009.12.14	RockYou Inc. (미국)
:	:	:	:
18	13,200,000	2011.11.25	Nexon Korea Corp(한국)

자료 : Open Security Foundation(http://www.datalossdb.org)

개인정보 유출 현황: 국내

- 유진호,지상호,임종인(2009)에 의하면 2005년 – 2007년 사이 개인정보 유출사고의 누적 피해자 수는 7천만 명, 손해배상금 추정액은 약 11조 원

〈국내 개인정보 유출사고 손해배상금 추정액〉

(단위 : 명, 억원)

	주소정보	주민번호	금융정보	민감성 정보	합계
사고 수	28	73	28	15	144
피해인원	37,050,968	27,149,916	6,169,484	8,421	70,378,789
배상금	37,048	54,300	18,508	59	109,915
사고당 배상금	1,323	743	661	4	763

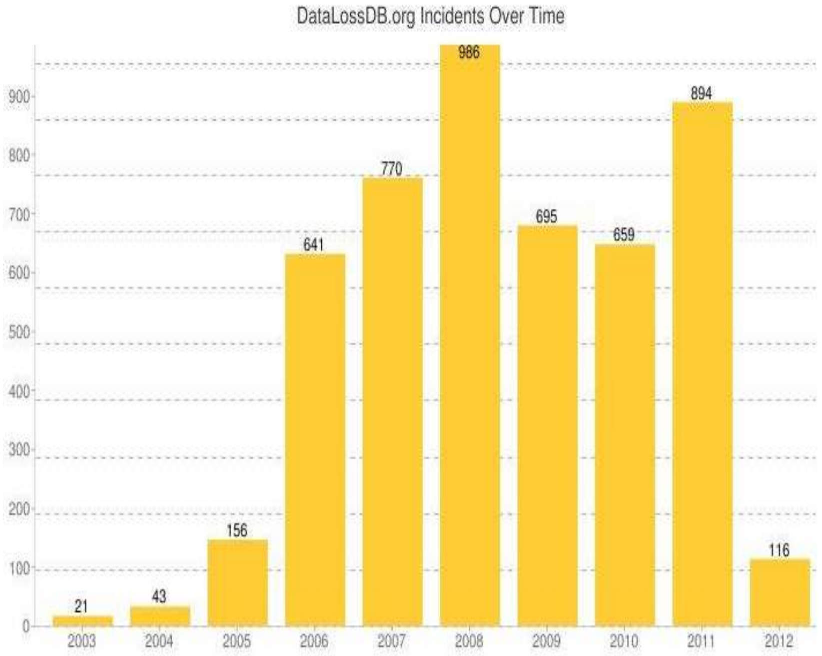
자료: 보험연구원(2011) 재인용, 원자료 유진호, 지상호, 임종인(2009)
주: 3개년 누적 수치

개인정보 유출 현황: 해외

❖ 2006년 이후 개인정보 유출사건 빈도가 증가하였으며, 유출정보 규모 또한 확대되는 추세

〈전세계 개인정보 DB 유출 추이〉

(단위 : 건)



자료 : Open Security Foundation(http://www.datalossdb.org)

- PGP/Ponemon의 분석에 의하면 주요국의 정보 유출사고 당 평균비용은
  - ✓ 미국: 675만 달러
  - ✓ 영국: 256만 달러
  - ✓ 독일: 344만 달러
  - ✓ 프랑스: 253만 달러
  - ✓ 호주: 183만 달러
  - ✓ 평균: 343만 달러

로 추정됨. (2009년 기준, 미국달러로 환산)

개인정보 유출 현황

- 전세계적으로 개인정보 유출 피해 건수 및 규모가 확대되는 추세
- 이러한 추세는 계속 될 것이며 Cyber Risk에 대한 노출은 확대될 것으로 예상됨.
  - 향후 디지털 정보량의 비약적 성장과 정보 활용 패턴의 변화
  - 클라우드 컴퓨팅 등 컴퓨터를 이용한 사업의 증가

국내 관련 제도 : 개인정보보호법

❖ 개인정보보호 관련 법률

구분	공공기관법	정보통신망법	신용정보법	전자금융거래법	개인정보보호법
입법일	1994.1.7	2001.1.16	1997.12.31	2007.1.1	2011.3.29
주무부처	행정안전부	방송통신위원회	금융위원회	금융위원회	행정안전부
적용대상	국가행정기관 지방자치단체 교육기관 기타공공기관	정보통신서비스제공자 집적통신시설업자 통신과금사업자 준용사업자	신용정보업자	전자금융업	공공기관, 민간사업자 (정보통신망법, 신용정보법 적용대상 제외)
유출사고 보고	정보주체가 침해사실신고(행안부)	침해사고신고 (방통위, 진흥원)	-	-	**-정보주체에 통지 의무화** -침해사실 신고
분쟁해결	개인정보보호심의위원회	개인정보분쟁조정위원회	-	금융분쟁 조정위원회, 소비자분쟁 조정위원회	개인정보분쟁조정위원회
피해자 구제	-	-손해배상청구권 인정 (입증책임전환) -책임보험가입의무화	-손해배상 책임 규정 (입증책임전환) -보험가입의무 없음	-손해배상책임(입증책임전환, 책임제한) -보험 또는 공제가입의무화	-손해배상책임(입증책임전환, 책임제한) -보험가입의무 없음

국내 관련 제도 : 개인정보보호법

❖ 개인정보보호법의 주요내용

장	절	조
제1장 총칙		목적, 정의, 개인정보보호원칙, 정보주체의 권리, 국가 등의 책무, 다른 법률과의 관계
제2장 개인정보보호 정책의 수립 등		기본계획의 수립 등, 시행계획의 수립, 개인정보보호위원회, 보호위원회의 기능, 자료제출요구, 개인정보호보지침, 자율규제의 촉진 및 지원, 국제협력
제3장 개인정보의 처리	제1절 개인정보의 수집, 이용, 제공 등	개인정보의 수집 · 이용, 개인정보의 수집제한, 개인정보의 제공, 개인정보의 제공제한, 개인정보를 제공받은 자의 이용제공제한, 개인정보의 파기, 동의를 받는 방법,
	제2절 개인정보의 처리제한	민감정보의 처리제한, 고유식별 정보의 처리제한, 영상정보처리기기의 설치운영제한, 업무위탁에 따른 개인정보의 처리제한, 영업양도 등에 따른 개인정보의 처리제한
제4장 개인정보의 안전한 관리		**안전조치의무, 개인정보처리방침의 수립 및 공개, 개인정보 관리책임자의 지정, 개인정보파일의 등록 및 공개, 개인정보의 영향평가, 개인정보의 유출통지**
제5장 정보주체의 권리보장		개인정보의 열람, 개인정보의 정정삭제, 개인정보의 처리정비, 권리행사의 방법 및 절차 등, 손해배상책임(37조)
제6장 개인정보분쟁조정위원회		설치 및 구성, 위원의 신분보장, 위원의 제척기피 · 회피, 조정의 신청 등, 처리기간, 자료의 요청 등, 조정 전 합의 권고, 분쟁의 조정, 조정의 거부 및 중지, 조정절차
제7장 보칙		적용의 일부 제외, 금지행위, 비밀유지, 의견제시 및 개선권고, 침해사실의 신고, 자료제출 요구 및 검사, 시정조치, 고발 및 징계권고
제8장 벌칙		

해외 관련 제도 : 미국

❖ 관련 법규

- 포괄적인 개인정보보호법제가 제정되어 있지 않으며 다양한 개별법과 자율규제를 중심으로 법적 대응이 이루어짐.
  - ✓ 공공부문 : Privacy Act(1974)가 대표적
  - ✓ 민간부문 : Fair Credit Reporting Act(1970), Health Insurance Portability and Accountability Act(HIPAA 1996), Children’s Online Privacy Protection Act(1999), Gramm-Leach-Bliley Act(1999) 등
- 각 주별로 독자적인 제도 마련, 민간기업에서의 자율규제와 가이드라인 운영
  - ✓ 개인정보유출고지법(Data Breach Notification Law)

해외 관련 제도 : 미국

❖ 개인정보유출고지법(Data Breach Notification Law)

- California State Law SB 1386 (2003)이 시작
- 개인정보 유출 시 구체적인 손해배상책임을 규정하지 않고 있으나, 사고 시 본인이 직접 고지하여야 하는 의무조항 때문에 개인정보유출 관련 보험시장이 성장하게 되는 계기 마련
- 법 도입 후 유출사고 통계가 급격히 증가

〈개인정보유출고지법 도입 주 현황〉

(단위 : 건)

	2003	2005	2007	2008	2009
도입한 주	1	19	39	45	46
유출사고건수	-	157	446	656	498

해외 관련 제도 : EU

❖ EU 지침: 공공부문과 민간부문을 포괄적으로 규제

- 개인 데이터 취급에 관해 비교적 엄격한 규정
  - ✓ 데이터 내용에 관한 원칙(6조)
  - ✓ 데이터 처리의 정당성의 기준(7조)
  - ✓ 민감성 데이터의 처리 제한(8조)
  - ✓ 데이터 주체에 제공되지 않으면 안 되는 정보(10,11조)
  - ✓ 데이터 주체의 접근권(12조)
  - ✓ 처리의 기밀성 및 안정성(16.17조)
  - ✓ 집행권한을 가지는 감독기관의 설치(28조)
- 각 국은 개인정보관련 법률 재정비 및 보험제도 도입

해외 관련 제도 : EU

❖ 유럽 주요국의 개인정보보호 법제 개요

국가	포괄법	관련 기관
영국	1998년 정보보호법	개인정보위원회(Information Commissioner's Office)
독일	2001년 연방정보보호법	BfD(Bundesbeauftragter fur den Datenshutz)
프랑스	정보처리, 정보파일 및 개인의 자유에 관한 1978년 1월 6일의 법률78-17호(2004년 8월 6일의 법률 제2004-801호에 의해 개정)	CNIL(Commission nationale de L'informatique et des Lobertes)

Cyber 보험시장

❖ Managing Cyber Risk

- Avoiding the risk
- Retaining the risk
- Mitigating the risk
- Transferring the risk

Cyber 보험시장

- Cyber Insurance (Cyber Risk Insurance):

"insurance contracts between insurance companies and enterprises or individuals covering financial losses incurred through damage or unavailability of tangible or intangible assets caused by computer or network-related incidents." (Anderson et al., 2008)

Cyber 보험 시장 : 미국

❖ 보장범위

- 정보 손실 및 유출에 대한 책임 (liability for loss or breach of the data)
  - ✓ 개인정보 관리 실패에서 발생한 계약자의 배상책임 관련 변호 및 합의 비용
- 유출 대응을 위한 개선 비용 (remediation costs to respond to the breach)
  - ✓ 조사, PR, 고객에 대한 공지, 신용감시 등을 포함하는 정보 유출에 따른 대응 비용
- 법 또는 규제에 의해 징수된 벌금 및 처벌에 대한 보장
  - ✓ 조사, 변호, 벌금 및 처벌에 대한 합의 관련 비용

Cyber 보험 시장 : 미국

❖ 연간수입보험료 추정치

- 2010년 연간 수입보험료는 8억 달러로 추정
- 2009년 연간 수입보험료는 6억 달러
- 2008년 4.5억~5억 달러

❖ Pricing

- 아직 초기 단계로 연성시장 형성
- 최근 개인정보유출고지법 시행에 따라 보수적 요율 산출 적용

❖ 판매회사

- AIG, Chubb, Hiscox, Legion Indemnity Company, Lloyd's, Marsh, St.Paul, Zurich north American Financial Enterprises 등

Cyber 보험 시장 : EU

❖ EU 국가들의 경우에도 개인정보보호관련 배상책임보험시장은 초기 단계

❖ 판매 회사

- ACE Europe, Hoscox, Lloyd’s, Marsh, Park Insurance, Services, Zurich North American Financial Enterprises 등이 관련 상품 취급

❖ 최근 개인정보 유출사고에 대한 체계적인 대책 마련하기 위해 ENISA(European Network and Information Security Agency) 출범

Cyber 보험 시장: 국내

❖ 보험상품 현황

<개인정보유출 관련 주요 보험상품 현황>

구분	상품명	주요 보상 내용	가입대상
의무 보험	전자금융거래배상책임보험	해킹 또는 전산장애 등으로 금융거래 피해를 본 고객이 입은 손해를 보상	금융기관 및 전자금융업자
	공인전자문서보관소 배상책임보험	전자문서보관 등의 업무수행과 관련하여 위법한 행위로 이용자에게 손해를 입힌 경우 손해를 보상	공인전자문서보관소
	집적정보통신시설 사업자 배상책임보험	집적정보통신시설의 멸실, 훼손, 그 외 운영장애로 발생한 피해를 보상	집적정보통신시설 사업자
임의 보험	개인정보유출배상책임보험	보험에 가입한 기업이 개인정보 유출을 당한 가입 고객으로부터 손해배상청구 소송을 당했을 때 발생하는 손해를 보상	온라인 쇼핑몰 등 고객정보를 다루는 업종
	e-Biz 배상책임보험	피보험자의 인터넷 및 네트워크 활동에 기인하여 타인에게 손해를 가함으로써 피보험자가 제3자에게 부담하여야 할 법률상의 손해를 보상	온라인 쇼핑몰 및 인터넷 개발업자 등

Cyber 보험 시장: 국내

❖ 보험 실적

- 국내에는 전자금융거래배상책임보험, 개인정보유출배상책임보험, e-biz배상책임보험 등 금융회사의 디지털 리스크 전가 상품이 있으나 담보금액이 낮거나 가입률이 매우 저조

〈원수보험료〉

단위: 천원

연도	전자금융거래배상책임보험	개인정보유출배상책임보험	e-Biz 배상책임보험
2005	-	681,616	684,647
2006	94,000	1,045,633	651,831
2007	1,654,830	779,760	318,793
2008	1,427,701	783,975	210,023
2009	1,589,297	648,819	293,843
합계	4,765,828	3,939,803	2,159,137

자료: 회사자료, 보험연구원(2011)에서 재인용

✓ 전자금융거래배상책임보험: 4년 누적 보험료는 약 48억 원

✓ 개인정보유출배상책임보험: 5년 누적 보험료는 약 39억 원

✓ E-Biz 배상책임보험: 5년 누적보험료는 약 22억 원

Cyber 보험 활성화 방안

Cyber 보험 활성화의 장애요인 (ENISA, Bohme, Majuca et al.)

- 양질의 계리 데이터 부족
- 리스크관리자, 고위 경영진의 해당 리스크에 관한 인식 부족
- 사이버 손실에 대한 계량화의 어려움
- 사이버 손실에 대한 설명의 불확실성

- ENISA(2008)은 의무보험제도 도입, 정부 재보험, 보험료 차별 금지, 금융시장에 사이버리스크 전가 수단의 확충, 보험가입 유도를 위한 인프라 구축 등을 제안

Cyber 보험 활성화 방안

국내 Cyber 보험 시장 활성화의 장애요인

- Cyber Risk 또는 개인정보유출 리스크에 대한 인식 부족
- 배상금 지급사례가 드묾.
- 배상을 받기 위해 피해여부를 소비자가 입증해야 함.
  - 피해자의 보험금직접청구권이 인정되나 보험금을 받기 위해서는 가해자의 귀책사유와 손해와의 인과관계를 입증해야 함.
- 2011년 제정된 개인정보보호법은 정보주체에게 정보유출사실을 통보하도록 되어 있어 배상청구가 용이해질 전망

Cyber 보험 활성화 방안

제도적 활성화 방안

- Cyber Risk 관리 인식제고 및 홍보 강화
  - 자율적 관리를 통해 최소의 개입으로 리스크관리 효율성 확보
- 법제화에 의해 가입 강제
- 공시제도 활용
  - 기업의 Cyber Risk 관리 수준을 공시하여 소비자가 확인할 수 있도록 하고 기업에게도 리스크관리 유인 제공

Cyber 보험 활성화 방안

민영보험회사의 역할

- ❖ 사이버리스크 배상책임보험제도에 적극적으로 참여
- ❖ 민영보험회사의 전문성 활용
  - 해당 리스크관리를 위한 다양한 상품개발
  - 손해사정 기법 개발
  - 리스크 분산기법의 다양화 등을 통해 구체화
- ❖ 경제적인 보험요율제도 제공

감사합니다

참고

❖ 개인정보 유출 추이: 해외

〈전세계 개인정보 DB 유출 사건 및 기록 현황〉

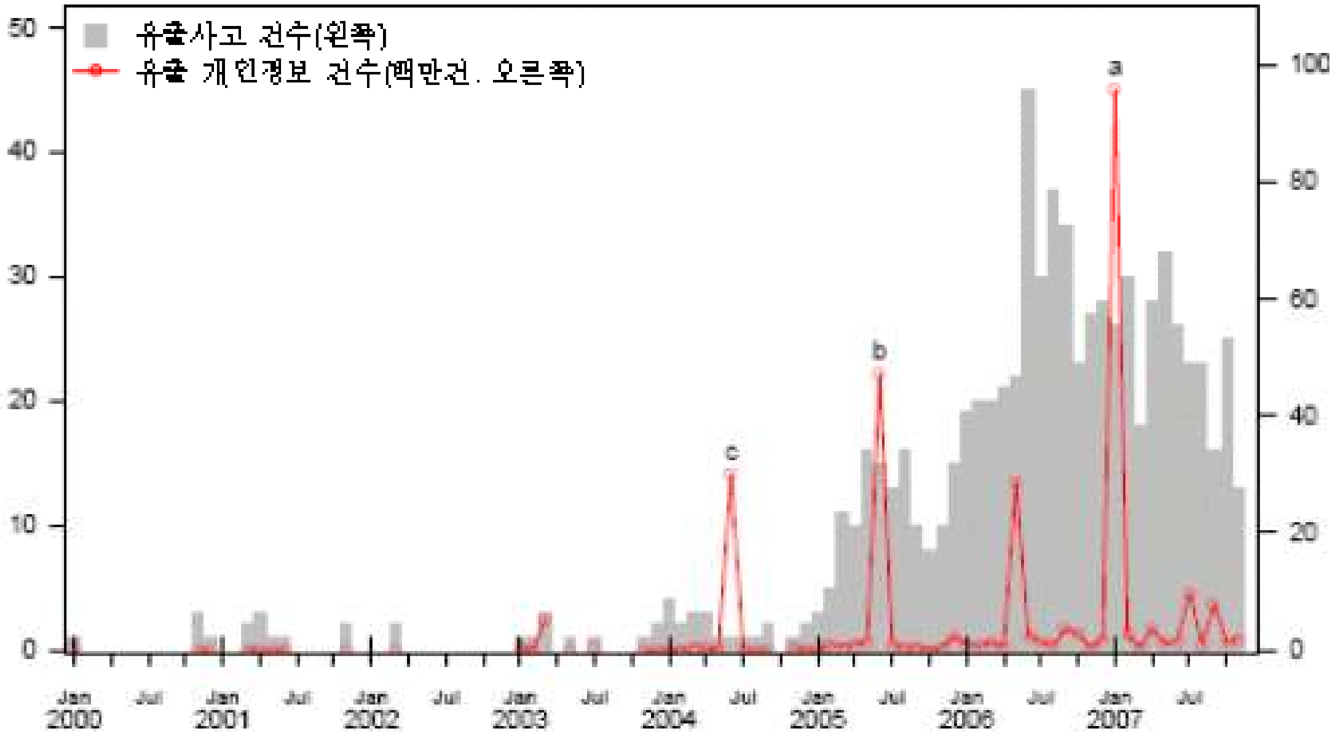
(단위 : 건, 개)

	2001	2003	2005	2007	2009
유출사건	17	14	140	489	436
유출정보	199,674	7,055,450	55,988,256	165,192,571	218,756,349
건당 유출정보	11,745	503,960	399,916	337,817	501,734

자료 : Open Security Foundation(http://www.datalossdb.org)

참고

<미국의 개인정보유출 추이>

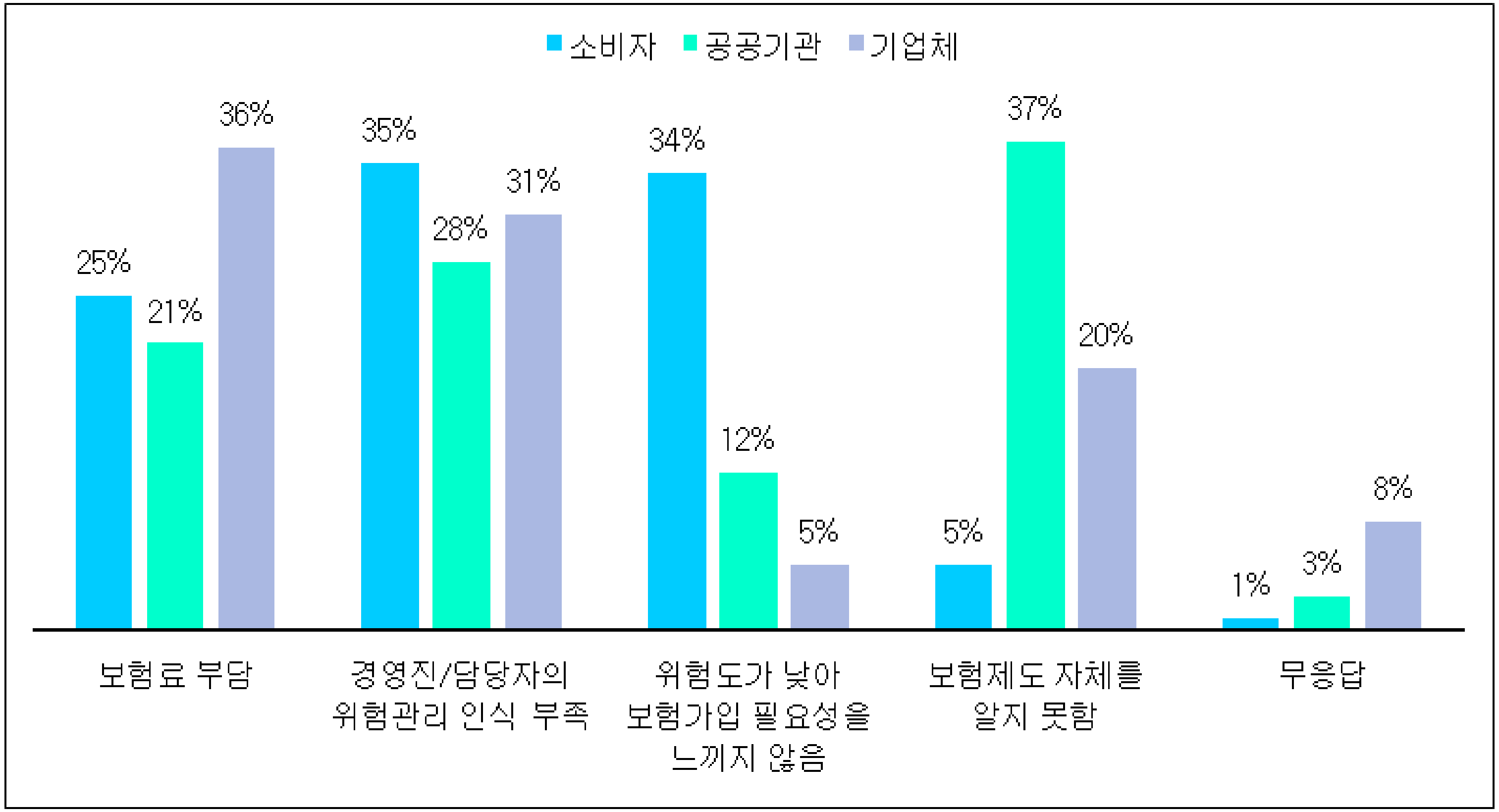


자료: Anderson et al. (2008)
주 : a) TJX Inc, b) Cardsystems, c) America Online

참고

❖ 보험가입 활성화 방안

<보험 미가입 이유>

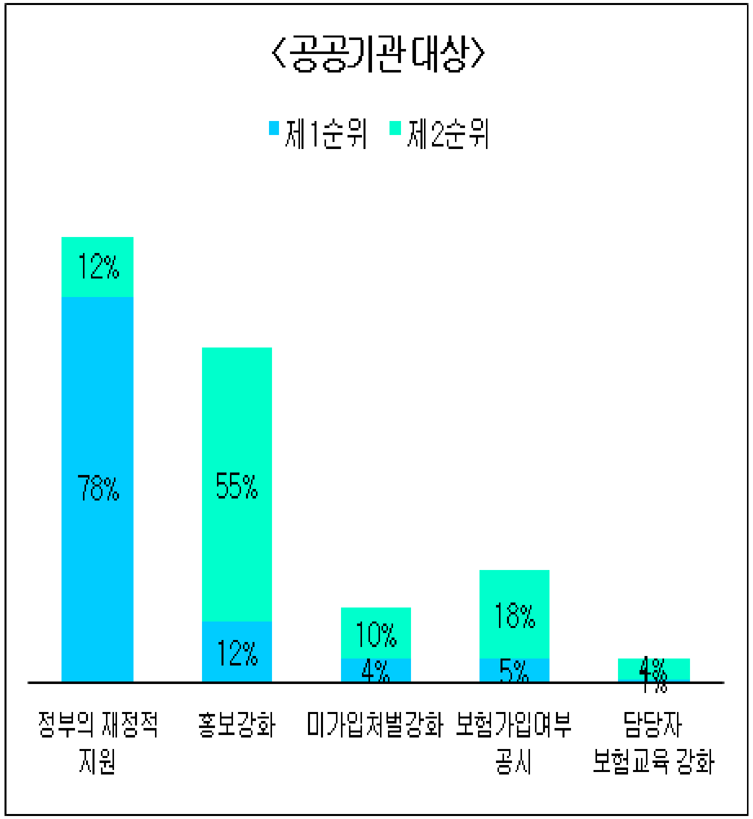


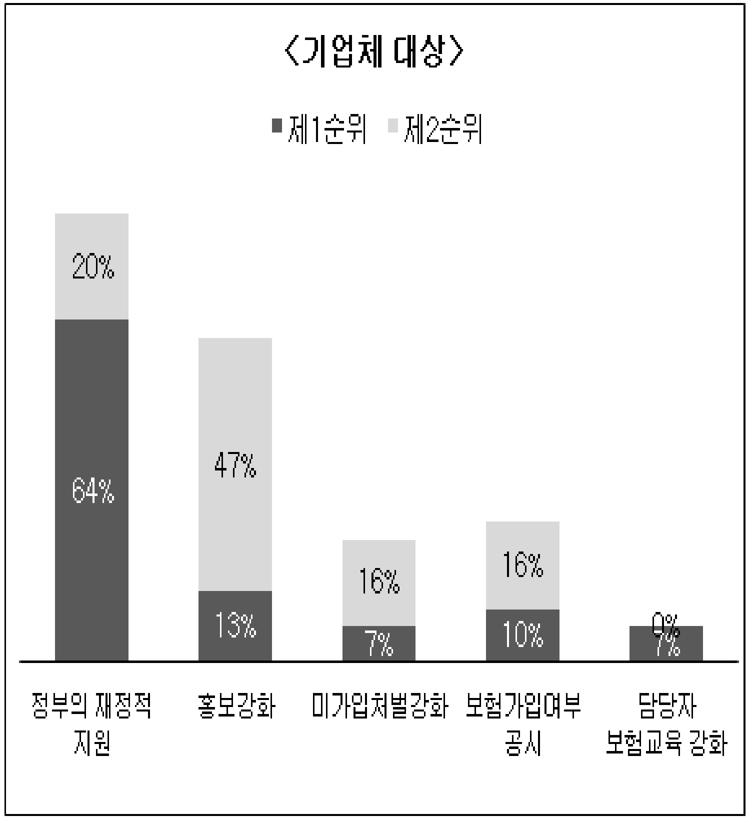
자료: 보험연구원(2011)

참고

❖ 보험가입 활성화 방안

<가입 활성화 방안_공공기관, 기업체>





자료: 보험연구원(2011)