

금융분야 개인정보 유출 재발방지 종합대책 주요내용

2014. 12.



금융감독원

목 차

I 재발방지 종합대책 마련 경과

II 재발방지 종합대책의 주요 내용

III 종합대책 관련 핵심 추진 과제

IV 종합대책 후속조치 이행

1. 재발방지 종합대책 마련 경과

- ❖ 금융위·안행부·방통위 등 **유관기관 합동**으로 개인정보유출 재발방지 근본대책 마련을 위한 「**금융회사 고객정보 정상화 TF**」가동(1.17.)
- ❖ 사고의 신속한 수습 및 안정화를 위해 재발방지대책의 큰 틀 및 주요골자인 「**금융회사 고객정보유출 재발방지대책**」 발표(1.22, 관계부처 합동)
- ❖ 불법정보 유통에 대한 국민 불안 해소를 위해 「**개인정보 불법유통·활용 차단 조치** (TM등 비대면 영업제한, TM대출모집인 경로 확인 등) 즉각 실시(1.24)
 - 엄격한 적법성 확인을 전제로 TM영업부터 재개를 허용하는 「**TM 등 비대면 영업 제한 관련 후속조치**」 발표(2.4)
- ❖ **3개 카드사**에 대해서는 개인정보 유출 책임을 물어 법정 최고한도인 **3개월 영업 정지 처분**(2.16)
- ❖ 국회 국정조사 과정의 논의사항 및 그간 대책 등을 반영하여 **종합적인 개인정보 강화 및 재발방지 방안 마련 및 발표**(3.10)

2. 재발방지 종합대책의 주요 내용

1. 수집정보의 필요최소화

- 개인정보 수집 최소화를 위한 가입서식 및 동의서 개정
 - 현재 30~50여개인 수집정보 항목을 필수항목(6~10개)과 선택항목으로 구분 · 최소화
 - 선택항목 동의는 “계약 체결에 필수적이지 않음”을 충분히 고지하고, 선택항목 동의 거부에 따른 불이익이 없도록 함
 - 사생활 침해 소지가 있는 결혼기념일, 종교, 배우자 및 가족정보는 원칙적 수집 금지

2. 주민번호 과다노출 관행 개선

- 당분간 금융회사의 주민번호 수집 · 이용은 불가피하나, 금융거래시 대부분의 서식에서 주민번호란을 삭제하여 노출을 최소화
 - 최초 거래시에만 전자단말기 직접 입력(Key-in), 신분증 사본 제공 등을 통해 주민번호를 수집
 - 이후 거래에는 주민번호 기입 없이 신분증, 인증시스템 등을 통해 신원확인절차만 거침
- 수집한 주민번호는 내부망에도 암호화하여 보관 ('16.1월부터 시행)
- 주민번호 불법활용 · 유출시 일반 개인정보 유출보다 가중제재

2. 재발방지 종합대책의 주요 내용

3. 지주그룹내 계열사 및 분사시 고객정보 이용 제한

- 고객 사전동의 없이 계열사 보유정보를 제공받아 외부영업에 이용하는 것을 원칙적 금지 (신용위험관리 등 내부경영관리 목적의 계열사간 정보공유는 허용)
- 지주사는 자회사 고객정보관리를 주기적으로 점검하고, 시정조치사항을 감독당국에 보고
- 분사시, 원칙적으로 자사고객이 아닌 개인정보는 이관 금지, 불가피하게 이관시는 자사 고객정보와 분리하여 엄격히 관리

4. 제3자 정보제공의 구체화

- 포괄적 정보 동의를 제한하여 “계약 체결에 필수적인 제3자”와 “선택적인 제3자”를 구분하여 동의
- 제공되는 정보의 내용, 이용목적, 제공되는 업체명 및 업체수, 제공기간 및 삭제 계획을 구체적으로 적시
- 제공기간은 “최소한의 기간”을 구체적으로 적시하고, 파기계획도 구체적으로 안내

2. 재발방지 종합대책의 주요 내용

5. 모집인 등의 불법정보 활용시 퇴출

- 불법유통정보를 활용한 대출모집인, 보험설계사 등에 대해서 즉시 전속계약을 해지
- 계약 해지된 대출모집인 등의 동일 영업행위 금지 (재등록 5년간 제한→사실상 금지)
- 대출모집인의 규정위반 등의 이력을 관리하는 “통합관리시스템” 구축

6. 무차별 비대면 방식의 개인정보 활용 엄격화

- 마케팅 목적의 문자전송(SMS)은 원칙적 금지 (별도 동의를 받거나, 기존계약 유지·관리 경우는 제외)
- 전화·이메일 등 비대면 영업에 대한 엄격한 통제방안 마련 (전화상담시 소속회사, 연락 목적, 정보획득경로 등을 사전에 명확히 안내)
- 보이스피싱, 불법사금융 등에 이용된 전화번호 차단, 발신번호 조작방지 등 관련대책 추진

2. 재발방지 종합대책의 주요 내용

7. 필요한 기간만 엄격히 보관 후 파기

- [1단계] 거래종료 후에는 원칙적으로 필요한 정보(식별정보, 거래정보 등) 만 보관하고 즉시 (3개월내) 파기
 - 현재 거래중인 고객정보와 분리하여 보관 (1단계 보안조치)
- [2단계] 거래종료 후 5년이 경과한 정보는 원칙적 모두 파기
 - 다만 법률상 의무이행 등을 위해 보관이 불가피한 경우는 “엄격히” 별도 관리 (2단계 보안조치 : 별도 DB보관, 업무상 필수인원만 접근)
 - 정보 재사용시 사전통지 의무화(영업목적 사용 제한)

8. 제3자에 제공된 정보통제 : 정보파기 및 확인의무

- 제3자와 개인정보 제공 계약시, 구체적 이용기간, 파기계획, 불이행시 패널티 등 명시
- 제3자가 이용기간 경과 후 정보를 삭제하였음을 금융회사가 확인토록 의무화 (파기확인 요청 및 파기확인서 징구)
- 제3자제공정보 관리실태를 CEO 등에 주기적으로 보고

2. 재발방지 종합대책의 주요 내용

9. 신용정보 주체의 권리 강화

- 본인정보 이용·제공현황 조회 요청권 : 고객이 본인 신용정보의 이용·제공현황을 확인할 수 있는 조회시스템을 금융회사별로 구축
- 연락중지청구권 : 금융협회 공동으로, 금융회사의 영업목적 연락에 대해 고객이 수신거부의사(Do not call)를 밝힐 수 있는 시스템을 구축
- 본인정보 파기요청권 : 고객이 거래종료 후 본인정보 보호 요청시, 파기 및 보안조치를 취하고 그 결과를 즉시 통보
- 본인정보 조회중지 요청권 : 고객 요청이 있는 경우, 명의도용 의심되는 신용조회를 일시 중지하고 고객에 지체없이 통지

10. 지속적 점검 및 평가

- 금융회사는 신용정보 관리·보호, 내부통제 현황 및 정보보호 관련 정책을 담은 “연차 보고서”를 작성하여 자체 점검
- “연차보고서”는 CEO, 이사회 등에 보고하고 금융당국에도 제출하여 CEO 등의 책임 강화

2. 재발방지 종합대책의 주요 내용

11. 모집업무 위탁(대출모집인 등) 관련 관리강화

- 모집인에게 고객정보 제공시 개인식별정보는 암호화
- 모집인은 “정보활용 · 파기 관리대장”을 작성하고 ,금융회사기 주기적 점검
- 금융회사는 모집인의 계약 승인시 “모집경로를 확인”하여 적법정보 활용 여부를 확인
- 모집인이 정보유출 · 불법정보 활용시 금융회사에도 엄정한 책임(과징금 부과) 추궁
 - 정보제공절차 준수, 모집경로 확인의무 등 주의의무를 다한경우 면책 가능

12. 사후적 제재 대폭 강화

- 불법정보 활용시 관련매출액의 3%한도까지 “징벌적 과징금” 부과
 - 관리소홀로 인한 정보유출시에는 일정금액(50억원)을 상한으로 설정
- 개인정보 유출 · 불법활용시 형벌수준을 금융관련법 최고수준(10년이하 징역)으로 상향
- 정보유출방지 주의의무 위반시 과태료수준 대폭 강화(600만원→5천만원)
- 금융회사 임직원 제재, 영업정지 등 기관제재도 보다 엄격히 이루어지도록 개선

3. 종합대책 관련 핵심 추진 과제

가. 대책 세부 가이드라인 및 지침 마련

- ❖ 대책의 원활한 이행을 위한 세부가이드라인 및 지침을 마련하고 금융회사에 대한 교육 실시
 - 주민번호 과다노출관행 개선 모범기준, 제3자 정보제공 구체화 가이드라인, 비대면 영업 제한 가이드라인 등 추가적으로 필요한 세부 가이드라인 및 지침 마련
 - 특히 개인정보의 파기에 대해서는 업무별로 파기 또는 보존필요성을 면밀히 검토하여 기준을 마련하고, 파기에 따른 문제가 발생되지 않도록 각별히 유의

나. 금융 IT · 사이버 보안 강화

- ❖ 외주용역 및 사이버해킹 등을 통한 정보유출을 차단하도록 보안강화대책 수립 및 불시점검을 위한 “기동점검반” 운영
 - 외주용역 일일 체크리스트 마련, IT실태평가제도 개선, 불시점검 계획 수립 및 시행

3. 종합대책 관련 핵심 추진 과제

다. 금융회사의 추진현황 점검·관리

- ❖ 금융협회 및 금융회사의 이행사항을 지도하고, 이에 대한 점검체크리스트 마련 및 점검 실시 등을 통해 이행현황 관리
 - 개인정보 수집 서식 및 동의서 개선, 불필요한 정보 파기, 정보유출대응매뉴얼 마련, 연차보고서 제출 등 대책 이행사항을 지도하고 점검 실시
 - 대출모집인 통합 관리 시스템, 본인정보이용현황 조회시스템, Do Not Call 시스템 등 전산시스템 구축이 필요한 사항도 구축대상 및 절차 등 기준을 제시하고 진행사항을 관리

라. 불법정보의 활용 및 유통 차단조치

- ❖ “개인정보 불법유통 감시센터” 및 “시민 감시단”을 적극 운영하고 수사기관과 협조하여 불법 정보유통을 근본적으로 차단
 - 금감원 내 “불법사금융 피해센터”를 확대 개편하여 “불법유통 감시센터”를 운영중(14.1월~)
 - 금감원, 시민 합동으로 약 150명이 참여하는 시민감시단 출범(14.2월~)
 - 불법행위에 사용된 전화번호를 적발하여 신속히 이용정지하는 등 범죄피해 예방강화

3. 종합대책 관련 핵심 추진 과제

마. 무분별한 모집업무 및 TM영업에 대한 제한조치

- ❖ 대출모집인, 보험설계사 등에 의한 무분별한 모집업무 및 TM활동을 엄격히 제한토록 금융회사 지도 및 모집인 교육
 - 불법적인 대출사기, 보이сп이스, 스미싱 등에 속지 않도록 금융회사에 대한 홍보활동을 지속적으로 전개
 - 무차별적인 문자전송(SMS) 및 e-mail, 전화 등 비대면 영업행위를 엄격히 제한토록 통제장치 마련 및 금융회사 지도

바. VAN사에 대한 감독기능 구축

- ❖ 대책에 따라 새롭게 금감원 감독·관리 대상에 포함되는 VAN사에 대한 효과적인 감독체계 및 관리방안 구축
 - VAN사의 IT안전성 확보, 신용정보 보호 등에 대한 검사를 실시하고, VAN사 검사 과정에서 VAN대리점에 대해서도 관리실태 확인
 - 카드가맹점 단말기를 IC단말기로 조속히 전환토록 적극 유도하고, 카드사를 통하여 간접적인 관리 수행

4. 종합대책 후속조치 이행

❖ 종합대책의 효과적인 이행을 위하여 금융권 실무자TF 구성(3.19)

- 세부기준 마련 및 이행상황의 주기적인 점검,관리

- 주관 : 금융위원회 서민금융과
- 간사 : 금융감독원 개인정보보호단 (현재 IT금융정보보호단)
- 반원 : 금융감독원 각 감독국, 각 금융협회(중앙회) 등
- 운영기간 : '14. 3. 19. ~
- 운영과제 : 종합대책 **이행상황 점검**, 금융권 **의견수렴** 및 **업권별 세부기준 마련** 등

❖ 종합대책이 차질없이 이행될 수 있도록 금융회사의 적극적인 참여 필요

- 각종 개인정보 수집 서식 및 동의서 개편
- 주민번호 등 개인정보의 수집 · 이용 최소화
- 개인(신용)정보의 적절한 파기 및 보관
- 연락중지청구서비스(Do not call) 운영 및 본인정보 이용 · 제공시스템 구축 등

Thank You !
