「금융분야 데이터 활용 및 정보보호 종합방안」
세부추진방안 ❶

금융분야 개인정보보호 내실화 방안

2018. 5. 11

금 융 위 원 회

목 차

Ⅰ. 추진 배경

□ 그간 **개인정보보호를 위하여 다각적인 노력**을 경주해 왔으며, 그 결과 **주요국에 비해 강한 정보보호 규제**가 도입·시행중

○ 특히, **'14년 신용카드사 정보유출사고** 이후 **정보의 수집·이용·제공 전반**에 걸쳐 **높은 수준의 규제**가 도입

- 한국의 정보보호규제는 **아시아에서 가장 강한** 수준이며, 특히 정보제공 동의제도는 전세계적으로도 강한 수준 (BBC news, '13.6월)
- 한국의 정보보호 규제수준은 **조사대상 OECD 주요국 중 가장 높은 수준**으로 정보활용에 큰 제약요인 (Analysys Mason, '14년)

□ 다만, 아직까지 **정보주체가 체감하기에 충분한 수준의 보호가 이루어지지는 못한다**는 지적

○ 다각적인 규제에도 불구, **지능정보화가 심화**되면서 **스스로 본인정보를 통제·관리해 나가기 갈수록 어려워지는** 상황

○ **정보활용 동의**를 비롯한 정보보호 제도가 **지나치게 복잡하게 운영**되어 정보주체의 권리가 **실질적으로 보장**되지는 **못하고 있음**

○ **정보주체 스스로도** 사생활 침해 등을 우려하면서도 실질적인 **정보보호 노력은 소홀히 하는** 경향도 존재('프라이버시의 역설')

□ 이에 따라 **데이터 활용에 대한 국민 불신이 심화**되고 **관련 규제가 강화**되는 **악순환**

* **국민신뢰 저하** → 정보보호규제 강화 → 형식적 운영으로 정보주체의 실질적 권리 보호 미흡 → **국민신뢰 저하**

○ **제도 운영의 경직성** 등으로 빅데이터 분석 등 **금융권 데이터 활용**을 통한 **4차 산업혁명 대응**에도 **걸림돌**이 된다는 평가

➡ **정보주체를 실질적으로 보호**하고, 데이터 활용에 대한 **국민신뢰**를 **제고**해 나가기 위해 **정보보호 제도의 내실화**가 필요

Ⅱ. 금융분야 개인정보보호 현황

1 개인정보 자기결정권의 의의

◈ 금융분야 개인정보보호는 **'개인정보 자기결정권'**을 중심으로 고유한 보호체계가 형성 ※ **(참고1)** 개인정보보호 논의의 흐름

□ 개인정보가 **언제, 누구에게, 어느 범위까지 알려지고 이용되도록 할 것**인지를 **정보주체 스스로 결정**할 수 있는 권리

○ 헌법상 **일반적 인격권**(§10), **사생활의 비밀과 자유**(§17) 등을 이념적 기초로 하는 **독자적 기본권으로 인정** (헌법재판소)

※ 최근 **헌법개정안**은 개인정보자기결정권을 기본권으로 **명문화** (§22②, "모든 사람은 자신에 관한 정보를 보호받고 그 처리에 관하여 통제할 권리를 가진다.")

○ 소극적 권리인 **사생활보장권**뿐만 아니라, 본인 정보를 **자율적으로 통제할 수 있는 적극적 권리**를 포함

※ "프라이버시란 단순히 타인에게 자기 정보가 없는 상태라기보다는, **'자기 정보에 관한 적극적인 통제권'**을 의미한다" - Charles Fried, 예일大

□ 개인정보 자기결정권은 **다른 기본권과의 관계, 데이터활용의 공익적 필요성** 등을 종합적으로 감안하여 **구체화**되는 권리

○ 타인의 **알권리, 표현의 자유**, 공유·활용을 통한 **사회 경제적 효율성** 등 데이터 활용의 다양한 목적이 균형있게 감안될 필요

○ 특히, 최근에는 개인정보가 가지는 **다차원적 속성을 인정**하고 **정보 유형별로 다른 접근*이 필요**하다는 인식이 확산

* (예) 사상·정치적 선호 등은 사생활 보장권적 성격을 가지나, 전화번호·주소 등 공개를 전제로 한 정보의 경우 자율적 통제권에 가까운 성격

□ **금융분야**의 경우, **고객 신용정보의 공유·활용**을 전제로 하는 **산업적 특성*** 등을 감안하여 특유한 **정보보호체계가 형성**

* 금융회사는 고객정보를 활용한 여신심사 등을 전제로 대출 등 금융상품을 제공
→ 금융분야 개인신용정보는 '개인'을 '신용사회'로 연결해주는 기능 수행

참고 1 개인정보보호 논의의 흐름

◈ 개인정보보호 논의는 **소극적 의미의 프라이버시권**에서 **자기정보의 적극적 통제·결정권** 등으로 **확대·진화**

1. 초기 논의 : '홀로 있을 권리'(a right to be let alone)

□ **프라이버시권**은 미국에서 **"홀로 있을 권리"**로 처음 소개된 후(1879, Thomas Cooley), **독자적 법적권리**로 논의(1890, Warren & Brandeis)

○ 사적 영역에 대해 **'타인으로부터 간섭을 받지 않을 권리'**로 인식

○ 주로 **공권력 등에 의한 정보의 부정유용** 등 **불법행위에 대항하는 개인의 권리**로서의 성격이 강조

2. 정보화 도래 이후 : '개인정보 자기결정권' 개념 도입

□ **국내외 판례***를 통해 '**개인정보 자기결정권**'이 **인정**되면서, 프라이버시권은 **본인정보를 통제하는 적극적 권리**로 확대

* 독일 '인구조사판결'(독일 헌법재판소, '83년)에서 최초로 인정

○ **산업화·정보화** 등의 진전에 따라 **유통·활용**될수록 **사회적·개인적 효용**이 증대되는 **정보의 본질적 특성이 부각**

○ '개인정보' 그 자체보다는 **'정보주체의 본인정보에 대한 결정·통제권'에 대한 보호**가 강조

3. 최근 논의 : 정보주체의 '보다 적극적·능동적인 권리' 부각

□ **빅데이터 등 정보환경이 급격하게 변화**하면서 정보주체의 **보다 능동적인 권리 보장**이 필요하다는 인식이 확산

○ 아울러, 사업자뿐 아니라 **개인 스스로 본인정보를 적극적으로 관리·활용**할 수 있는 권리로 **프라이버시 개념이 확장**

※ 실용주의적 프라이버시 이론 (Daniel J. Solove, 조지워싱턴大 교수)

○ 프라이버시에 대한 인식은 **시대, 장소, 문화적 관습**에 따라 **상이**하며, **개별적인 정보 유형별**로 **다른 접근**이 필요

○ 프라이버시권은 **시대적 맥락, 상충하는 다양한 가치를 조화롭게 고려**하여 구체적 보호수준을 정할 필요

2 국내 제도 현황

◈ 우리의 정보보호법제*는 개인정보 자기결정권의 핵심수단인 **동의제도**를 비롯하여 **다양한 제도**를 도입하여 시행중

* 개인정보보호는 일반법인「개인정보보호법」외에 분야별 특별법으로 「신용정보법(금융)」, 「정보통신망법(정보통신)」에서 규율 중

1 **사전적 선택·결정권**: 정보활용에 관한 **"동의권"**

○ **개인정보의 수집·이용·제공**을 위해서는 **사전적**으로 **정보주체**에게 **이용목적·제공기관** 등을 알리고 **동의**를 받아야 함

2 **보조적 권리**: **정보 열람청구권, 제공·이용 사실조회권**

○ 정보주체는 금융회사 등이 보유한 **본인정보의 열람 청구** 가능

○ 금융회사 등은 정보주체가 **본인정보의 이용·제공 현황을 확인할 수 있는 시스템**("조회시스템")을 구축·제공해야 함

3 **사후적 통제권**: **정정·삭제·처리정지** 요구권, **동의 철회권** 등

○ 정보주체는 일정한 경우* 외에는 **본인 정보를 정정하거나 삭제**할 것을 금융회사 등에게 요구할 수 있음

* (정정·삭제 거절사유) 해당 정보가 법령상 수집대상인 경우 (처리정지 거절사유) 법령상 의무이행, 계약이행 등을 위해 불가피한 경우

○ 마케팅 등 목적으로 한 **제3자 제공 동의는 철회 가능**하며, **마케팅 목적의 연락에 대한 중지 청구권**("Do-not-call")도 보장

4 **권리구제·제재수단**: 엄격한 **행정제재, 민·형사상 책임** 등

○ 정보유출 발생시 지체 없이 **정보주체에게 통지, 금융위에 보고**토록하고, 유출기관에 대해 **행정·민형사상 엄중 제재***

* **(행정)** 과징금(관련매출액의 3%한도), 과태료 등, **(형사)** 10년이하 징역 또는 1억원 이하 벌금, **(민사)** 법정·징벌적손해배상(손해 3배한도) 등

○ **권리침해 행위**에 대한 **집단적 분쟁조정**(ADR) 및 **침해의 중지·금지를 요구**하는 **단체소송**까지 허용

Ⅲ. 평가 및 문제점

1. 우리의 정보보호 규제는 주요국에 비해 엄격한 수준

□ **정보활용 동의규제**의 경우, **엄격한 사전동의 원칙**하에 **필수/선택동의가 구분**되는 등 여타 국가들에 비해 **보호수준**이 **강한 편**

※ 주요국 정보활용 동의제도 비교

- **(미국) 필수/선택을 구분**하여 **필수적 정보**는 **동의를 요하지 않고 선택적 정보**의 경우 **사후 거부제도***(Opt-out)를 원칙으로 함

  * 개인정보 이용에 대한 고지(프라이버시 안내서 송부) 후 일정기간(약 30일)내 정보주체가 거부권(옵트-아웃권)을 행사하지 않으면 정보이용이 가능

- **(EU) 사전동의제**이나, **필수/선택구분이 없어** 거래체결을 위해서는 **거래에 필수적이지 않은 정보***까지도 **동의가 불가피**

  * (예) 마케팅 목적, 데이터 분석 목적을 위한 정보활용 등

<미 국>	< E U >	<한 국>
사후거부(Opt-out)	**사전동의(Opt-in)**	**사전동의(Opt-in)**
+	+	+
필수/선택 구분	필수/선택 미구분	**필수/선택 구분**

□ 정보주체의 **사후통제권, 정보보호 관련 권리구제·제재수단** 등도 **주요국에 비해 보호 강도가 매우 높은** 수준

- **미국·EU 등**의 경우, **부정확한 정보**에 한해 **정보주체의 삭제·정정요구권**을 인정 * 미국의 경우 동의 철회권도 불인정

- **정보유출시 손해배상**의 경우에도 '14년 카드사 정보유출사태 이후 **EU 등 주요국에 없는 강력한 규정***이 도입

  * (i) 실제 손해액의 3배한도의 **징벌적 손해배상제도**
  (ii) 손해액 입증 없이도 법원 판결로 손해액을 정하는 **법정 손해배상제도**
  (iii) 고의·과실이 없었음을 정보이용 기업이 입증하여야 하는 **입증책임전환**

2. 강한 규제에도 불구, 정보주체의 실질적 권리 보호는 미흡

□ 정보주체의 **인지적, 구조적 한계*** 등으로 **법상 보장된 정보주체의 권리**가 **실질적으로 보호되지 못하는** 상황

* **'프라이버시의 역설('Privacy Paradox')'**
: 프라이버시 침해 가능성을 우려하면서도, 자신에게는 실제 피해가 없으리라 믿거나(제3자 편향), 프라이버시를 양보하여 얻게 되는 편익이 더 크다고 생각하여(위험-보상 평가) 프라이버시 보호를 위한 실제 행동에는 나서지 않는 현상

cf) 정보화진흥원 실태조사 결과('14)
- **개인정보 침해를 경험**한 인터넷이용자들 중 **37.7%만 대응조치**를 취함
- **개인정보 처리사항**에 관한 **정보를 제공받을 권리**는 **38.2%**, **개인정보 정정·삭제·파기요구권**은 **22.4%**만 인지

□ 특히, 개인정보 자기결정권의 핵심적 구현수단인 **동의제도가 형식화**되어 **'알고하는 동의(Informed consent)'**가 **이루어지지 못함**

○ 정보주체가 정보활용 내역 및 프라이버시 침해 정도 등에 대해 **정확하게 알고 동의하는 비율은 매우 낮은** 상황*

* **온라인 약관**을 자세히 읽고 서명하는 비율은 **4%** (서울대 산학협력단, '14)

○ 기업은 **정보주체로부터 더 확실한 동의**를 받는 데에만 주력하고 정보주체에 대한 **효율적 정보제공 노력은 소홀**

※ Facebook 개인정보 유출의혹 사례("Cambridge Analytica scandal")

▪ **Facebook**은 **이용자들의 정치적 성향 등 민감 정보**를 데이터 연구기관에 **대량으로 판매**하면서,

- 개인정보 제공 사실이 잘 드러나지 않도록 **'정보제공 설명 및 동의양식'을 복잡하게 개편**('12년)

▪ 파이낸셜타임즈 등 외신은 **동의제도**가 성가신 절차와 복잡한 양식 등으로 **불투명한 정보활용 관행의 은폐수단**이 될 수 있음을 지적

* FT(3.27일) : "**동의는 (기업의) 책임을 조각하지 않으며**, 거대 IT 기업은 정보보호와 신뢰회복을 위해 보다 책임성 있게 대처해야 함"

3. 환경 변화 등을 감안한 적극적 권리보호 논의는 부족

□ **빅데이터 환경**에서 **새롭게 등장한 개인보호 이슈**에 대한 **논의는 부족**한 상황

○ ①**개인에 대한 평가**가 ②**개인정보**를 기초로, ③**기계적·자동적**으로 이루어지는 **'프로파일링'**의 확산으로 **정보주체 소외 우려**

* **EU의 일반개인정보보호법**(GDPR, '18.5월 시행)에서는 프로파일링 결과에 대한 정보주체의 이의제기 등 **적극적 대응권**을 도입한 바 있음

□ 개인정보를 금융회사 등 기업뿐 아니라, **정보주체가 스스로 관리·활용**할 수 있는 여건은 미흡

* EU GDPR에서는 자산관리 서비스, 보다 유리한 금융상품 등을 제공 받는데 본인정보를 활용할 수 있도록 **개인정보 이동권** (Data portability)**을 도입**

4. 금융권 정보활용·관리 실태에 대한 상시적 감독체계 부재

□ 현재는 **상시적 검사·감독 체계가 미흡**하여 정보유출 등 이상징후 발생시 **개별적, 사후적으로 점검·감독**하는 수준

* 전산상 보안에 대해서는 「전자금융법」상 취약점 점검 평가가 도입되어 있으나 정보보호 규제 전반에 대해 점검하는 체계는 미흡

◈ **형식적으로 강한 규제수준**에도 불구하고 정보주체에 대한 **내실 있는 보호가 이루어지지 못하는 상황**

○ 특히, **정보보호 책임**이 정보를 활용하는 기업 및 감독책임이 있는 정부보다는 **정보주체에게만 전가**되고 있다는 지적

➡ **정보보호 규제를 보다 실질적으로 정비**함으로써 **데이터 활용에 대한 국민신뢰를 제고**해 나갈 필요

Ⅳ. 개선 방안

< 기본 방향 >

◈ **개인정보의 수집·활용 전과정**에서 **투명성**을 높이고 **정보주체를 보다 내실있게 보호**

○ **정보활용 동의제도 개선**을 통해 동의내용에 대해 명확하게 '**알고하는 동의**(Informed consent)' 여건 마련

○ **동의과정**에서 **기업의 설명의무 등 책임을 강화**하고, 정보주체로서 **개인의 과도한 정보확인 부담**을 경감

◈ **새로운 유형의 권리침해 가능성**에 선제적으로 대응하고, **적극적·능동적 권리보호 제도를 도입**

○ **빅데이터 결과** 등에 대해 **정보주체가 적극적으로 대응**해 나갈 수 있도록 **권리 보장**('프로파일링 대응권' 강화)

○ 보다 나은 금융서비스를 제공받기 위해 **본인정보를 능동적으로 관리·활용**할 수 있는 여건 마련('개인신용정보 이동권' 도입)

◈ **개인정보 유출 및 오남용** 등으로부터 **정보주체를 안전하게 보호**할 수 있도록 **금융회사 등과 정부의 관리노력** 강화

○ **금융권의 개인정보 활용·관리실태**에 대한 **체계적이고 상시적인 점검·감독 시스템**을 구축

○ **정보보호 우수기업 인증마크제** 도입, **모범사례 공유** 등을 통해 **시장 규율도 강화**

※ 추후 **국민 신뢰, 사회적 합의** 등을 토대로 **초연결 시대**에 걸맞게 **정보보호 규제를 보다 합리화하는 방안**도 검토*

* (예시) **사물인터넷** 등 기술적으로 사전 동의제도를 적용하기 어려운 영역에 대해서는 **미국식 사후거부제**(Opt-out) 도입을 허용

1 정보활용 동의제도 실질화

(1) 정보활용 동의서의 실질화·단순화

□1 금융회사 등이 **수집·이용**하거나 **제3자에게 제공**하는 정보의 내용을 **단순화·시각화**하여 **정보주체에게 전달**

* (유사사례) **페이스북**은 회원들이 최근 본인 정보 활용내역 확인, 정보 활용 중단 요청 등을 쉽게 할 수 있도록 **'Privacy Shortcuts'**을 제공('18.3월)

○ 이를 위해 **동의서 양식개정**을 **우선 추진**하되, 추후 「신용정보법」을 개정하여 **동의서 형식 관련 사항을 법제화***

* 현행 신정법은 동의 내용, 동의 방식 등에 대해서는 규정하고 있으나, 정보주체 인지 등과 관련한 동의서 양식의 기본원칙 등은 미규정

cf) **이른바 '경품응모권 1mm 글씨 고지' 사례**

▪ 유통업체 A사는 **1mm 크기 글씨**로 **개인정보제공 동의**를 받고 이를 **제3자(보험사)에게 판매**한 바 있음 (대법원은 **'부정한 수단을 통한 개인정보 동의'**로 보아 **위법**하다고 판시('17.4월))

⇨ 동의서 양식개정은 **기업의 정보제공의 책임을 강화하여** 이러한 **불투명한 정보수집·활용 시도**를 **사전적으로 방지**

□2 **수집·이용·제공되는 정보의 내용**에 대해 정보주체에게 **요약 정보**를 **우선 제공**하도록 함

○ 다만, **고객이 요구**할 경우 **상세 정보**도 함께 제공하도록 함

*** (유사사례) 자본시장법상 간이투자설명서 제도**

- 집합투자증권 모집·청약 권유 시 고객이 투자설명서를 별도로 요청하지 않을 경우 간이투자설명서로 대체 가능 (다만, 간이투자설명서를 교부하는 경우 투자설명서를 별도로 요청할 수 있음을 알려야 함)

➡ 동의과정에서 동의를 하는 **정보주체의 확인부담을 줄이고,** 동의를 받아 정보를 활용하는 **금융회사 등의 책임을 강화**

(2) 정보활용 동의서 등급제 도입

□ 정보활용 동의시 정보제공에 따른 **사생활 침해 위험 및 소비자 혜택** 등에 대한 **종합적 평가등급**을 산정·제공

○ 개인에 대한 정보제공기능 외에도, **불필요한 정보수집 최소화** 등 **금융회사 등의 개인정보보호 노력**도 유도

<동의서 등급제 도입방안(예시)>

• **(등급 산정 기준) 정보활용 영향도, 수집정보 민감도** 등을 감안

구분 (가중치)	**수집·이용 동의 시**
수집정보 민감도 및 사생활 침해위험(50%)	· 수집 또는 제3자 제공정보의 범위 및 민감 정도 · 제공정보의 사생활 관련성 및 유출시 피해정도
정보활용 영향도(40%)	· 정보 제공기간, 이용 목적, 정보 활용에 따른 혜택
소비자 친화도(10%)	· 동의서 구성의 금융소비자 인지 및 이해 용이성

• **(등급분류) 적정, 비교적 적정, 신중, 매우 신중** 등 4단계로 부여

➡ **개인의 인지적 한계**를 **보완**하고, **금융회사의 자체노력 유도**

(3) 이용목적별·기관별 동의제도 도입 (※ 국정과제)

□ 정보주체가 정보활용 현황을 **활용목적별·기관별로 구분**하여 **개별적으로 동의여부를 선택**할 수 있도록 개선

* 현재는 활용목적과 기관을 동의서에 명시하기는 하나, 일괄 동의관행(무더기 동의)으로 정보주체의 선택권이 제약

○ 다만, 필수적 동의사항의 경우 선택권 확대 효과 보다는 동의 절차만 복잡하게 할 우려가 있어 **선택적 동의사항에만 도입**

- **필수적 동의사항**의 경우 동의항목을 세분화하기보다는 **정보제공의 실질화에 초점**을 두어 개선

➡ 개인의 **실질적 선택권을 보장**하되, 절차적 번거로움은 최소화

참고 2 현행 정보활용 동의서 양식

개인(신용)정보 필수적 동의서

※아래의 동의사항은 대출계약 및 유지를 위한 필수 사항입니다.

개인(신용)정보 필수적 수집·이용에 관한 사항

주식회사 귀하

귀사와의 (금융)거래와 관련하여 귀사가 본인의 개인(신용)정보를 수집·이용하고자 하는 경우에는 「개인정보 보호법」 제15조 및 22조, 제24조 「신용정보의 이용 및 보호에 관한 법률」 제32조, 제33조 및 제34조에 따라 동의를 얻어야 합니다. 이에 본인은 귀사가 아래의 내용과 같이 본인의 개인(신용)정보를 수집·이용하는데 동의합니다.

● 개인(신용)정보의 수집·이용 목적

계약의 체결, 유지, 이행, 관리, 개선, 신청 상품 및 관련서비스 제공, 법령상 의무이행, 신용질서 문란행위 조사, 분쟁처리, 전화상담업무, 민원처리, 본인여부 확인, 공증, 채권추심

● 수집, 이용할 개인(신용)정보의 내용

① **개인식별정보** : 성명, 주민(법인)등록번호, 사업자번호, 주민등록증 발급일, 연락처(휴대폰, 자택, 직장), 주소(자택, 직장), 이메일, 직장명, 부서, 직위, 직종, 소득구분, 성별, 국적, 운전면허번호, 여권번호, 외국인등록번호, 음성데이타, CI(연계정보 : Connecting Information)

② **신용거래정보** : 귀사 및 타 금융사의 본 거래 이전 및 이후의 대출, 보증, 담보제공, 신용카드, 할부금융 등 상거래 관련 거래의 종류, 기간, 금액, 이용한도 등 거래 내용을 판단할 수 있는 정보

③ **신용도정보** : 신용등급, 신용조회기록, 채무재조정약정, 연체, 부도, 대위변제, 기타 신용질서 문란행위 관련 금액, 발생·해소 시기 등 신용도를 판단할 수 있는 정보

④ **신용능력정보** : 재산, 채무, 소득의 총액, 납세실적 등 신용거래능력을 판단할 수 있는 정보

⑤ **공공기관정보** : 개인회생, 파산, 면책, 채무불이행자 등재 등 법원의 재판결정정보, 체납정보, 주민등록관련정보, 사회보험, 공공요금 관련정보, 행정처분에 관한 정보 등 본인 식별, 신용도 및 거래 능력을 판단할 수 있는 공공기관 보유정보

⑥ **기타 계약 및 서비스의 체결, 유지, 이행, 관리, 개선 등과 관련하여 본인이 제공한 정보**

※이하에서는 개인식별정보, 신용거래정보, 신용도 정보, 신용능력정보, 공공기관정보에 해당하는 각각의 개별정보 명칭은 생략합니다.

※CI(연계정보) : 주민등록번호를 대체하기 위하여 본인확인기관(나이스평가정보㈜등)에서 부여하는 개인식별정보

● 개인(신용)정보의 보유, 이용기간

거래 종료(채권채무 관계종료)일로부터 5년(단, 관련법령의 별도 규정이 명시되어 있는 경우 그 기간을 따름)

본인은 귀사가 상기 목적으로 다음과 같은 본인의 고유식별정보를 처리하는 것에 동의합니다.
– 고유식별정보 : 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호 동의함 □ 동의하지 않음 □

년 월 일 성명 : 서명 또는 (인)

본인은 본 동의서의 내용을 이해하였으며, 개인(신용)정보 제공·이용에 관한 고객 권리 안내문에 관하여 자세히 설명을 듣고 수령하였습니다.

년 월 일 성명 : 서명 또는 (인)

개인(신용)정보 조회에 관한 사항

「신용정보의 이용 및 보호에 관한 법률」 제32조 제2항 및 「개인정보 보호법」 제24조에 따라 귀사가 아래와 같은 내용으로 신용조회회사, 신용정보집중기관으로부터 본인의 신용정보를 조회하거나, 공공기관을 통하여 본인임을 확인하는 것에 대하여 동의합니다.

- **조회할 개인(신용)정보** : 개인식별정보, 신용거래정보, 신용도정보, 신용능력정보, 공공기관정보
- **조회 목적** : 계약의 체결, 유지, 이행, 관리, 개선
- **조회동의 효력기간** : 귀하가 상기 동의서를 제출한 시점부터 당해거래 종료일까지 상기동의의 효력이 유지됩니다. 다만, 이 계약이 성립되지 않는 경우 그 시점부터 동의의 효력은 소멸합니다.

본인은 귀사가 상기 목적으로 다음과 같은 본인의 고유식별정보를 처리하는 것에 동의합니다.
– 고유식별정보 : 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호 동의함 □ 동의하지 않음 □

년 월 일 성명 : 서명 또는 (인)

본인은 본 동의서의 내용을 이해하였으며, 개인(신용)정보 제공·이용에 관한 고객 권리 안내문에 관하여 자세히 설명을 듣고 수령하였습니다.

년 월 일 성명 : 서명 또는 (인)

참고 3 개정 정보활용 동의서 양식(案)

① **복잡한 정보제공 설명양식을 단순화**(원하는 고객에게는 상세설명도 제공)
② **동의서 등급제 도입**(적정/비교적 적정/신중/매우 신중 4등급으로 구분)
③ **정보활용기관-목적별로 구분**하여 동의(선택적 동의사항에만 적용)

2 다양한 개인정보 자기결정권 보장 강화

(1) 프로파일링 대응권 강화

◈ **EU 사례, 국내 법·제도적 여건** 등을 감안하여 **금융분야**에서 발생 가능한 **프로파일링**에 대한 **정보주체의 대응권**을 보장

□ **('프로파일링' 개념)** 개인정보의 **기계화·자동화**된 **처리**를 통해 개인의 **성격, 행태, 취향 등을 분석·예측**하는 행위

○ 최근 **빅데이터, 인공지능, 머신러닝** 등 **기술의 발전**에 따라 다양한 영역에서 **프로파일링이 빈번**하게 이루어짐

- **금융분야**에서도 통계모형·알고리즘에 의한 **개인신용평가** 외에도 **온라인 대출, 자동화된 보험료 산정** 등으로 확산 추세

○ **맞춤형 상품 개발, 효율적 고객관리** 등 산업적 측면에서 **프로파일링의 필요성**이 있으나,

- **무분별하게 이루어질** 경우 **정보주체의 권리가 침해**될 소지가 상존하는 만큼 **적절한 보완장치가 마련**될 필요

□ **(EU 규제사례(GDPR))** ①**프로파일링 과정·결과**의 **투명성을 제고**하고, ②**정보주체의 적극적인 대응권**을 보장

① **프로파일링의 근거·기준** 및 **개인에게 미치게 될 영향도** 등을 정보주체에게 **알기 쉽게 전달**토록 함

* "Data subject should be informed of meaningful information about the logic involved and significance and envisaged consequences" - GDPR 가이드라인('17.10)

② **프로파일링 근거·기준**에 대한 **정보주체의 의견표현·이의제기권** 보장, **맞춤형 마케팅** 등에 대한 **정보주체의 거부권** 도입

□ **(국내 제도현황) 정보주체 대응권 보장**을 위한 **제도 일부 도입**

○ **개인신용평가**와 관련하여, 일정한 경우 **설명요구·의견표현·이의제기권** 등 **정보주체의 대응권**이 도입

* 개인신용평가 결과에 따라 **금융거래를 거절**당한 경우, 본인 평가에 활용된 **정보 내역 및 정확성 확인 요구** 가능 (설명요구권)
* 개인이 **직접 본인의 긍정적 정보**(통신료, 사회보험료, 세금납부실적 등)를 신용조회사(CB사)에 제공시 **개인신용평가상 가점을 부여** (의견표현권)

○ 그밖에, 금융회사 등의 정보활용에 대해 **처리 정지·정정** 요구, **마케팅 거부권**("Do-not-call")등이 **일반적으로 보장**되고 있음

□ **(개선방안) 개인신용평가 관련 대응권**을 **확대·강화**하는 한편, 일정한 **금융거래**에 대해서도 **설명요구·이의제기권**을 **확대**

○ **(개인신용평가) 금융거래 거절 여부와 관계없이** 신용등급·점수에 관한 **설명요구·이의제기권*을 폭넓게 인정**

* 모든 개인에게 ① 개인신용평가 결과에 대한 설명요구권, ②평가의 기초정보가 부정확할 경우 정보 정정청구 및 ③ 평가 재심사 요구권 등

○ **(금융거래)** 빅데이터 분석 등 **자동화된 개인 평가**를 기초로 하는 **금융거래***에 대한 **개인의 적극적 대응권****을 도입

* (예) 신용카드사의 맞춤형 혜택 제공, 보험료 자동산정 시스템 등

** ① (설명요구권) 자동화된 개인 평가의 근거·기준 등에 대한 설명 요구
② (의견표현권) 평가상 혜택을 받기 위한 본인의 긍정적 정보 제출권
③ (이의제기권) 자동화된 개인 평가의 기초가 된 정보가 부정확한 경우 이의를 제기하고 평가 재심사를 요구할 권리

√(예시) : 보험료 자동산정 관련 설명요구권 사례

- A 보험사는 보험 가입자의 **주행습관 등 운전행태 정보**를 기반으로 **자동적으로 보험료를 산정**하는 자동차 보험을 판매하고자 함
- 고객이 설명을 요구하는 경우, A보험사는 **보험료 산정의 근거가 되는 운전행태**에 대해 **그래픽 등을 이용하여 알기 쉽게 설명**하고, 모바일 앱(App) 등을 통해 급제동·급가속 등과 **같은 주행 습관에 따른 보험료 변동**을 알 수 있는 **모의실험** 등을 제공해야 함

(2) 개인신용정보 이동권 도입

◈ **개인신용평가, 본인정보관리, 금융거래의 편의성 제고** 등에 활용할 수 있도록 **본인의 개인신용정보 이동권**을 보장

□ **(개념)** 정보주체가 본인의 개인신용정보를 보유한 기관으로 하여금 **본인정보를 제3자에게 이동**시키도록 할 수 있는 권리

□ **(활용사례 ①) 개인신용평가 개선 목적**으로 활용

○ **본인의 긍정적 정보**를 **CB사 및 금융회사**에 **전달**하여 **개인신용평가 및 여신심사** 등에 **유리하게 활용**

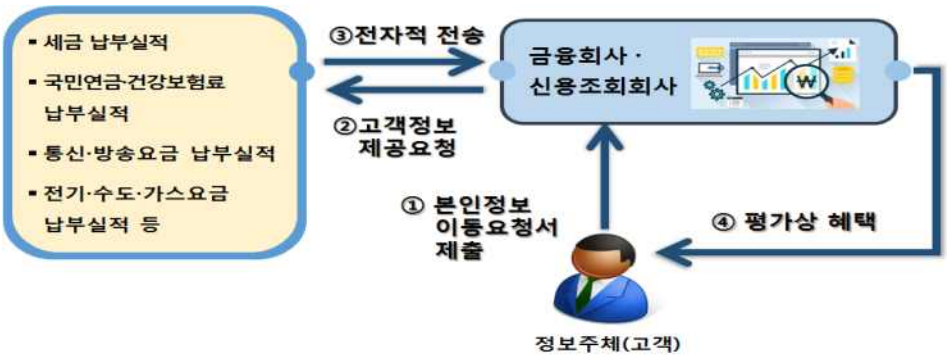
▪ 현재도 본인의 **긍정적 정보** 제공시 **평가상 가점제도**가 있으나, 개인이 **직접 주기적으로 정보를 수집·제출**해야 하는 등 절차가 번거로워 **활용도 미미** ('16.7월 시행 이후 **약 4.2만명** 활용중)

⇒ **개인신용정보이동권을 행사**하여 본인정보를 **전자적으로 전송**하게 함으로써 **지속적인 가점혜택**을 받을 수 있게 됨

√활용사례 (예시)

- **사회초년생 직장인 A씨**는 대출도 없고, 신용카드 사용내역도 없어서 CB사의 신용등급이 **6등급**이었다(**금융이력부족자**).
- 앞으로는 A씨가 CB사에 **본인정보 이동요청서**를 제출하면 CB사가 휴대폰 요금 및 국민연금 납부내역 등을 해당기관으로부터 정기적으로 제공받아 개인신용평가에 반영하게 된다.

→ A씨는 **최대 50점 가점**을 부여받아 신용등급이 **5등급으로 개선**되어, 보다 좋은 조건으로 전세금 대출이 가능해질 수 있다.



□ **(활용사례 ②) 본인정보관리서비스를 제공**받는 데에 활용

○ **다양한 기관에 분산**되어 있는 **본인 신용정보**를 **본인정보 관리업자에 제공**하여 **손쉽게 정보관리서비스**에 접근

<본인신용정보관리업 도입방안>

▪ 본인정보관리업자는 (i) **예금, 대출, 카드거래** 등의 정보를 망라하는 **본인 신용정보의 통합조회서비스**를 제공하고,

▪ (ii) 이를 기초로 **소비패턴, 위험성향 등을 파악**하여 **자산관리서비스** 제공 및 **맞춤형 금융상품 추천**

* 「금융분야 데이터활용 및 정보보호 종합방안」(3.19일)에서 주요내용 발표 (세부 추진방안은 **추후 별도 발표 예정**)

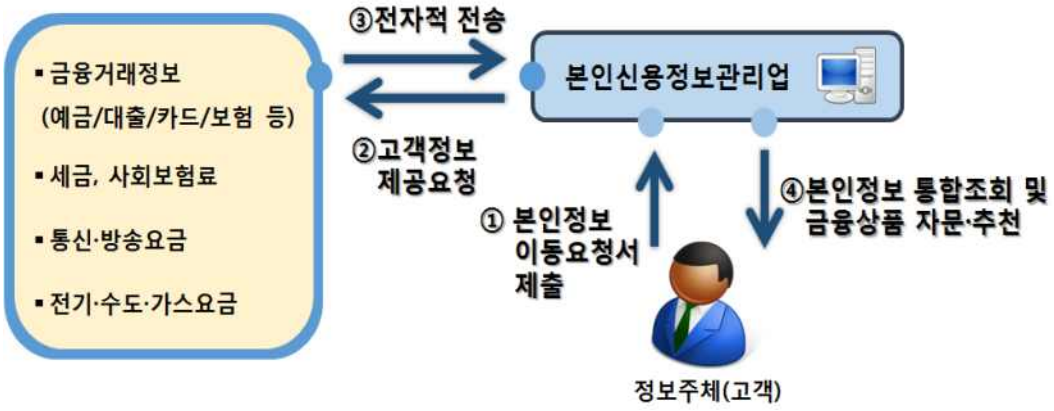
√활용사례 (예시)

• **회사원 A씨**는 재무관리를 위해 입출금 및 대출 원리금 납부내역, 카드사용내역, 휴대폰·국민연금·전기수도·가스요금 납부내역 등을 **일일이 해당 회사·기관의 홈페이지를 통해 확인**하고 있으며,

재무/투자상담 등 자산관리서비스를 받을 때에도 **해당 자료를 직접 챙겨서 투자자문회사에 제출**해야 하는 불편이 있었다.

• 앞으로는 **본인정보 이동요청서**를 본인신용정보관리회사(B사)에 제출하면 B사가 해당 정보를 보유한 기관에 요청하여 A씨의 신용정보를 정기적으로 전송받아, **A씨에게 한번에 보여줄 수 있으며(통합조회서비스 제공),**

A씨는 B사로부터 **저렴한 비용**으로 **신용카드 등 금융상품 추천, 주식/채권/펀드 등 투자자문, 지출/수입 관리** 등 **종합자산관리서비스**를 받게 된다.



3 금융권 정보보호 및 보안 강화

(1) 금융권 정보활용·관리 상시평가제 도입 (※ 국정과제)

□ **(현행)** '17년부터 **금융권 정보보호 운영실태**에 대한 **보고·점검 제도가 도입**되었으나, **조직·인력상 한계** 등으로 **형식적 수준***

* '17년부터 금융회사에 신용정보 관리·보호인을 지정토록 의무화 되었으나, 아직까지 단순 실적보고에 그치며, 취약점 평가 및 보완조치 의무 등은 부재

□ **(개선)** 금융권 정보활용·관리 실태에 대해 **상시적으로 점검**하는 **체계적인 감독시스템**을 구축

❶ **(평가체계)** ①**금융회사 자체평가***, ②**자율규제기구****의 **점검**, ③**금감원 검사** 등 **중첩적 평가체계**를 구축

* 금융회사내에 정보보호 자체평가반을 구성하여 평가내실화(외부 전문기관에 평가 의뢰 허용) → 신용정보 관리·보호인의 역할과 책임을 강화

** 금융분야 정보보호 관련기관으로 신용정보원·금융보안원 등 금융위 지정기관 (cf.「**개인정보보호법**」에서도 **개인정보보호 자율규제단체 지정제** 운용 (현재 대한병원협회, 대한약사회 등 14개 단체 지정)

《 금융분야 개인정보 활용•관리 실태 상시평가 수행체계 》

❷ **(평가대상)** 금융감독원 검사 대상 **전체 금융회사** (3,584개)*

* 금융지주(9), 은행(57), 저축은행(79), 여전사(98), 보험(62), 상호금융(2,258), 금투업자(799), 신용정보회사(29), 대부업자(193) ('17년말 기준)

❸ **(평가항목)** 신용정보법상 개인정보보호 관련 규정에 기초한 **8개 대항목* 및 72개 세부항목**

* ① 개인신용정보 수집·이용, ② 제공, ③ 처리위탁, ④ 안전한 보관, ⑤ 파기, ⑥ 신용정보활용체제 공시, ⑦ 내부통제, ⑧ 신용정보주체의 권리보장

❹ **(평가결과·피드백)** 자율규제기구는 **금융회사 자체평가**를 서면 점검하고 **결과를 점수화·등급화**하여 **금융당국에 제출**

- 금융당국은 평가결과에 기반하여 필요시 **현장점검, 테마검사** 등 실시하고 **취약부문 보완조치 등을 요구**

《 금융분야 개인정보 활용•관리 실태 상시평가 흐름도 》

❶ 금융회사는 자체평가반 및 외부 전문기관을 이용하여 자체평가를 실시

❷ 자율규제기구는 금융회사 자체 평가결과를 서면으로 확인(필요시 자료보완 요청)하고 이를 점수화·등급화하여 금융위/금감원에 제출

❸ 금융위/금감원은 자율규제기구의 점검결과를 바탕으로 필요시 현장점검·테마검사 등을 실시하고 취약부문 보완조치 등을 요구

(2) 인증마크 제도 도입 등 시장규율 강화

□ **일정기간**(예 : 3년이상) **상시평가 결과가 지속적으로 우수**하고 **개인정보 침해사고** 등이 없는 경우 **'안전성 인증마크' 부여**

○ **인증의 정당성을 확보**하기 위하여 **외부 전문가로 구성된 '인증심사위원회*'**를 **별도 운영**

* 금융위가 지정하는 자율규제기구내 설치·운영하는 방안 검토

※(유사사례) 개인정보보호 인증제도

- 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 개인정보법에 부합하는지 등에 관하여 인증 (인증기관 : 한국인터넷진흥원(KISA))

□ 금융회사 등에 **개인정보보호·관리계획**을 매년 **수립하여 시장에 공시**토록하고,

○ **자율규제기구**를 중심으로 **개인정보보호 교육** 등을 강화하여 **정보주체의 정보보호 중요성 인식 환기** 노력도 병행

□ **모범사례 발굴·공유**를 통해 **금융회사의 정보관리 강화** 유도

○ **정보보호 우수기관**의 정보 활용·관리 **모범사례**를 발굴하여 **전 금융권에 적극 공유** (개인정보보호 가이드라인 등 배포)

(3) 포괄적 조치명령권 도입

□ 금융위의 **금융회사, CB사 등의 정보 수집·이용·제공**에 대한 **포괄적 조치 명령권을 신설**

○ 대량의 **정보유출·침해사고** 등 **위기 발생시**에 **신속하고 체계적인 대응**을 통해 **규제 실효성 확보**

* 자본시장법(§416), 보험업법(§131) 등에서는 旣 도입

4 추가 검토필요 과제 : 사후거부제(Opt-out) 도입

◈ **금융환경 변화, 제도적 여건 및 사회적 합의 추이**를 보아가며 **사후거부제**(Opt-out)를 **단계적으로 도입**하는 방안도 검토

□ **4차 산업혁명 흐름**이 심화되는 가운데, **현행 정보활용 사전동의제**를 **일부 완화**해야 한다는 **지적**이 꾸준히 제기

○ 기술적 특성을 고려하지 않고 **사전동의제를 일률적으로 적용**할 경우 **사물인터넷**(IoT)* **등 관련 산업발전 저해** 우려

* 사물인터넷의 경우, 정보의 성격상 사후에 주기적으로 정보 활용내역을 통지하고 **거부권을 부여**하는 것이 **실효적 규제**방안

○ 특히, **미국**은 **사후거부제** 등 데이터 활용에 자유로운 법·제도 하에 **데이터 기반 혁신**이 활발히 이루어지고 있음

* **(참고 4)** 미국식 사후거부제 운용 방식

□ 다만, 사후거부제는 **개인정보 자기결정권 침해 소지**가 있는 만큼 **금융환경 변화** 등을 감안하여 **도입 여부를 검토**할 필요

○ **금융분야에 사물인터넷 등 신기술이 확산·도입**되는 추이*에 따라 기술혁신을 저해하지 않도록 **유연한 제도 설계** 검토

* (예) 최근 자산 포트폴리오 자동관리, 자율주행차 보험 등 IoT 활용 사례 증가

○ **해외 금융기관과의 역차별** 우려 및 **국내 금융산업 경쟁력 강화 필요성** 등을 감안한 **단계적 도입 방안***도 검토 필요

* (예) 금융지주회사 그룹내에서 영업상 이용목적으로 정보 공유시부터 도입하는 방안 등 (현재는 내부관리목적에 한해 사전동의 없는 정보공유 허용)

□ 아울러, **사전-사후규제 균형** 등을 감안한 **전반적인 규제체계 개선 논의**와 함께 **충분한 사회적 합의**를 거칠 필요

○ **추가적인 권리구제·제재수단**이 도입될 경우, 이에 상응하는 **사전규제 완화 방안**으로서 **사후거부제 도입**도 검토

참고 4 미국의 동의제도 운영 방식

1. 주요 원칙

□ **필수적 정보 제공사항*** ⇨ **동의를 요구하지 않음**

* 금융거래 체결을 위해 필수적으로 필요한 정보 외에도 **해당 회사의 마케팅을 위한 정보 이용**도 포함

□ **선택적 정보 제공사항*** ⇨ **사후 거부제도**(Opt-out)로 운영

* 제3자(계열사 및 비계열사)의 마케팅 목적을 위한 정보 전달

2. 실제 운영방식

1 **계약 당시**에는 정보제공 동의를 **요구하지 않음**

2 **거래체결 이후 우편, 전자메일** 등을 통해 '**프라이버시 안내서**(Privacy Notice)'를 제공

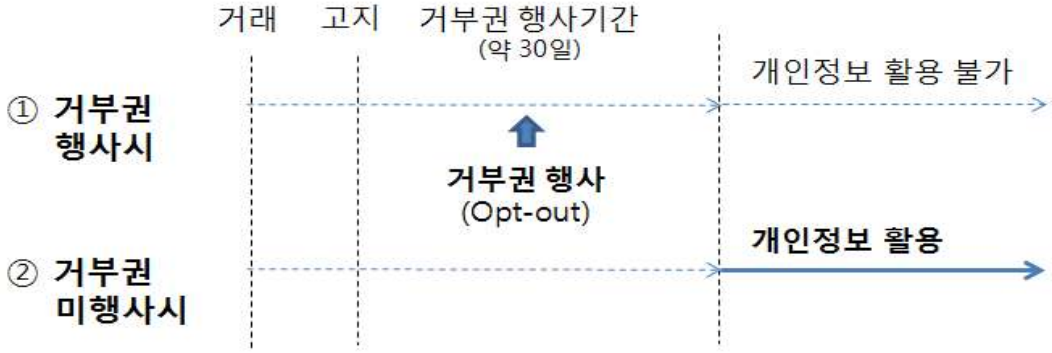
※ 프라이버시 안내서의 주요 기재사항

- (i) (**필수적** 동의사항) **정보 이용·제공 상세 내역**
- (ii) (**선택적** 동의사항) **거부권(Opt-out) 행사 기간 및 방법** 등

3 **선택적 동의사항**의 경우, **거부권 행사기간**(통상 30일)내 **거부권 행사가 없는 경우 정보 활용**

* 필수적 제공사항은 동의를 요구하지 않으므로 거래체결 당시부터 활용

<선택적 동의사항 정보 처리 절차>



Ⅴ. 향후 추진계획

□ 금년 상반기 중 가능한 방안부터 **조속히 추진**

○ **금년 상반기** 중 **「신용정보법」** 개정안이 **국회에서 논의될 수 있도록** 입법 노력 추진

○ 법 개정 이전이라도 **하위규정 개정** 등으로 추진이 가능한 과제는 **우선 추진**

〈과제별 추진일정〉

추진 과제		추진 일정
동의제도 내실화	1 요약정보 제공 등 정보제공 실질화	'18.下중 업권별 표준동의서 양식 개정 ('18년중 관련 신정법 개정 추진)
	2 정보활용 동의서 등급제 도입	
	3 이용목적별·기관별 동의제도 도입	
개인정보 자기결정권 강화	1 프로파일링 대응권 강화	'18년중 신정법 개정 추진
	2 개인신용정보 이동권 도입	
금융권 정보보호·보안 강화	1 금융권 정보활용·관리 상시평가제 도입	'18년중 실무안 마련 → '19년부터 시행 ('18년중 관련 신정법 개정 추진)
	2 정보보호 우수기관 인증마크제 도입 등	'18년중 신정법 개정 추진
	3 포괄적 조치명령권 도입	