

국내 금융보안 관련 주요 법령 (재생산 증강 생성(RAG) 및 LLM 튜닝용)

한국의 금융보안·개인정보보호 체계는 여러 법률과 규정을 통해 구성되어 있다. 여기서는 **데이터 보호, 사이버보안, 전자금융, 자금세탁방지(AML), 금융기관 실명 확인** 등 금융보안과 직접 관련되는 국내 법령을 정리하였다. 각 법령의 목적과 특징을 간략히 설명하고, RAG/LLM 튜닝 시 활용할 수 있도록 핵심 키워드를 표 형태로 정리하였다.

주요 법령별 설명

개인정보보호법(Personal Information Protection Act, PIPA)

- **개요** - PIPA는 대한민국에서 개인정보 처리와 보호를 **총괄**하는 기본법이다. 베이커맥킨지 자료에 따르면, PIPA는 개인정보 처리와 보호를 포괄적으로 규율하는 기본법으로, 다른 법률을 제정·개정할 때 그 목적과 원칙을 PIPA와 일치시켜야 한다 ¹. 2023년 9월과 2024년 9월에 주요 개정이 있었으며, 이후에도 세부 규정이 꾸준히 개정되고 있다 ².
- **범위** - PIPA는 정부 기관을 포함한 대부분의 조직에 적용되며, 2011년 9월 30일에 제정되었다. Ground Labs 블로그는 PIPA가 남한 시민의 개인정보를 수집·처리하는 거의 모든 조직(정부 포함)에 적용되는 매우 엄격한 법이라고 설명한다 ³.

신용정보의 이용 및 보호에 관한 법률(Credit Information Use and Protection Act, Credit Information Act)

- **목적** - 신용정보법은 금융권에서 **개인의 신용정보**를 수집·이용·제공하는 기준을 규정한다. 베이커맥킨지 자료에서는 이 법이 금융 부문에서 개인 신용정보의 이용과 보호를 주로 규율한다고 설명한다 ⁴. Ground Labs는 이 법이 신용평가를 위한 신용정보를 규제한다고 요약한다 ⁵.
- **특징** - 신용정보업의 건전한 육성과 신용정보주체의 권리를 보호하기 위해, 신용정보를 수집·이용·제공할 때 사전 동의를 요구하며, 신용정보회사에 대한 라이선스 제도(MyData 제도) 등을 포함한다.

위치정보의 보호 및 이용 등에 관한 법률(Location Information Act)

- **목적** - 위치정보법은 개인의 **위치정보**의 수집·저장·보호·이용을 규율한다. 베이커맥킨지는 위치정보법이 위치정보의 수집·저장·보호 및 이용을 규율한다고 밝혀 PIPA 보완적 역할을 한다고 언급한다 ⁶.

정보통신망 이용촉진 및 정보보호 등에 관한 법률(Network Act)

- **목적** - 네트워크법은 정보통신망의 이용 활성화와 정보보호를 목적으로 한다. 베이커맥킨지는 이 법을 주요 사이버보안 법령으로 명시한다 ⁷.
- **보안 의무** - 사이버보안 관련 자료에 따르면, 네트워크법 제VI장은 모든 **망서비스제공자**에게 네트워크 안정성 확보, 정보보호 사전점검, 최고정보보호책임자(CISO) 지정 등의 의무를 부과한다 ⁸. 또한 IoT 제품 제조사·수입자에게도 사이버 공격 대비를 위한 정보보호 지침 준수 의무를 부과한다 ⁹. 네트워크법은 통신사업자에게도 취약점 분석·평가 등 추가적인 보안조치를 요구한다 ¹⁰.

전자금융거래법(Electronic Financial Transactions Act, EFTA)

- **목적** - 전자금융거래의 **안정성과 신뢰성**을 확보하는 데 목적이 있다. 베이커맥킨지는 전자금융거래법을 핵심 사이버보안 법령으로 나열한다 ¹¹.

- **보안의무** - 사이버보안 자료에 따르면, 전자금융거래법 제33장은 금융회사나 전자금융업자에게 **전자금융거래 안전성 확보, CISO 지정, 전자금융 인프라 취약점 분석·평가** 등을 요구한다 ¹² . 이는 금융 전산망의 안전성을 보장하기 위한 핵심적인 조항이다.

정보통신기반 보호법(Act on the Protection of Information and Communications Infrastructure, Infrastructure Act)

- **목적** - 국가 및 금융·통신·교통·에너지 등 주요 **정보통신기반시설**의 보호를 위한 법률이다. 베이커맥킨지는 이 법을 주요 사이버보안 법령으로 소개한다 ¹³ .
- **보안의무** - 사이버보안 자료에서는, 이 법이 공공·민간 부문 핵심 인프라 관리기관에게 보호조치 마련, 주기적 **취약점 분석 및 평가**, 사고 발생 시 신속한 복구 조치 등을 요구한다고 설명한다 ¹⁴ .

공공데이터의 제공 및 이용 활성화에 관한 법률(Public Data Act)

- **목적** - 공공데이터의 제공과 이용을 촉진하기 위한 법률로, 데이터 활용 확대와 혁신 촉진을 목표로 한다. 베이커맥킨지는 이 법과 시행령을 주요 **비(非)개인정보** 법령으로 제시한다 ¹⁵ .

데이터산업 진흥 및 이용 활성화 기본법(Data Industry Act)

- **목적** - 데이터 산업의 육성과 데이터 이용 촉진을 위한 기본법이다. 베이커맥킨지는 이 법을 비개인정보 분야의 핵심 법령으로 소개한다 ¹⁶ .

특정 금융거래정보의 보고 및 이용 등에 관한 법률(금융거래보고법, Financial Transaction Reports Act - FTRA)

- **목적** - 자금세탁 및 범죄자금 조달을 방지하기 위해 금융기관에게 **거래정보 보고**와 **고객확인(CDD)** 등을 요구하는 법률이다.
- **주요 내용** - 한국금융정보원(KoFIU)에 따르면, 한국의 **자금세탁방지/테러자금조달금지(AML/CFT)** 체계는 금융거래보고법(FTRA)과 **테러자금금지법**에 기반하며, FTRA는 KoFIU의 법적 근거로서 금융기관에게 고객확인·의심거래보고(STR)·거액현금거래보고(CTR) 등을 의무화한다 ¹⁷ . 같은 자료는 법령과 시행령을 명시하며, FTRA가 예방적 조치의 기반이라는 점을 강조한다 ¹⁸ .

테러자금금지법 및 대량살상무기 확산금지법(Act on Prohibition against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction)

- **목적** - 테러자금 조달 및 대량살상무기 확산 자금 조달을 방지·처벌하기 위한 법률이다.
- **특징** - KoFIU는 이 법이 테러자금 조달 행위를 처벌하고, 금융위원회의 사전 승인 없이 특정 개인·법인·단체와의 금융거래를 금지한다고 설명한다 ¹⁸ . FTRA와 함께 한국의 AML/CFT 체계의 중요한 축을 이룬다.

금융실명거래 및 비밀보장에 관한 법률(Real Name Financial Transactions Act)

- **목적** - 금융거래의 **실명제**를 법제화하여 자금세탁과 부정거래를 예방하는 법률이다.
- **주요 내용** - BNP Paribas Korea에 따르면, 한국에서 금융기관은 금융실명법과 FTRA에 따라 **고객확인제도(CDD)**를 준수해야 한다. 금융실명법은 **익명계좌 개설 금지** 및 **고객의 실명 확인**을 규정하여 금융기관이 실명 여부를 확인하도록 요구한다 ¹⁹ . FTRA 개정을 통해 CDD 범위가 확대되었다는 점도 언급된다 ²⁰ . Ground Labs 역시 금융실명법을 금융기관에 적용되는 분야별 법령으로 소개한다 ²¹ .

국내 금융보안 관련 법령 키워드 정리

주요 법령 (한글/영문)	핵심 주제 키워드	관련 분야
개인정보보호법 (Personal Information Protection Act)	개인정보 처리, 정보주체 권리, 전면적 규율 ¹	데이터 프라이버시, 금융보안 전반
신용정보법 (Credit Information Use and Protection Act)	개인 신용정보 보호, MyData, 신용정보업 규제 ⁴	금융 데이터, 신용평가
위치정보법 (Location Information Act)	위치정보 수집·보호, 저장·이용 규제 ⁶	위치기반 서비스, 개인정보
정보통신망법 (Network Act)	네트워크 안정성, CISO 지정, 정보보호 사전점검 ⁸	사이버보안, IT 서비스
전자금융거래법 (Electronic Financial Transactions Act)	전자금융거래 안전성, CISO 지정, 취약점 분석 ¹²	전자결제, 핀테크
정보통신기반 보호법 (Infrastructure Act)	국가/금융 인프라 보호, 취약점 평가, 복구 조치 ¹⁴	핵심 인프라, 금융/통신
공공데이터법 (Public Data Act)	공공데이터 제공·이용 촉진 ¹⁵	비(非)개인 데이터 활용
데이터산업법 (Data Industry Act)	데이터 산업 육성, 데이터 활용 촉진 ¹⁶	데이터 경제, 혁신
금융거래보고법(FTRA) (Financial Transaction Reports Act)	AML/CFT, 고객확인 (CDD), 의심거래보고 (STR) ¹⁷	자금세탁방지, 금융기관 준법
테러자금금지법 (Act on Prohibition against the Financing of Terrorism and Proliferation of WMD)	테러자금 조달 금지, 제재 대상 거래 제한 ¹⁸	테러자금방지, AML/CFT
금융실명법 (Real Name Financial Transactions Act)	실명확인, 익명계좌 금지 ¹⁹	고객확인제도, 자금세탁방지

정리 및 활용 방안

- 국내 금융보안 법령은 **데이터 보호, 사이버보안, 전자금융, AML/CFT, 실명제** 등 여러 영역에 걸쳐 있다. LLM 튜닝 시에는 각 법령의 **목적, 주요 조항, 의무, 시행 연도** 등을 문서에 포함해 맥락을 풍부하게 할 수 있다.
- PIPA와 신용정보법·위치정보법 등의 **개인정보 관련 법령**은 금융기관의 데이터 처리 준수 기준을 결정하며, 전자금융거래법과 정보통신망법·정보통신기반 보호법 등의 **사이버보안 법령**은 전산망 안정성과 전자금융 인프라 보호 의무를 정한다.
- 금융거래보고법과 테러자금금지법, 금융실명법 등 **AML/CFT 관련 법령**은 자금세탁 및 테러자금 조달 방지를 위한 보고·감시·실명확인 제도 등을 규정한다 ^{17 19}.
- 이 법령 목록과 키워드는 문서 검색(RAG) 및 LLM 튜닝 시 유용한 인덱스 역할을 하며, 각 법령의 시행 시기와 관련 규정의 세부 내용까지 확장하면 보다 심층적인 학습 자료를 구성할 수 있다.

1 2 4 6 7 11 13 15 16 **Key Data & Cybersecurity Laws | South Korea | Global Data and Cyber Handbook | Baker McKenzie Resource Hub**
<https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/south-korea/topics/key-data-and-cybersecurity-laws>

3 5 21 **South Korea's Privacy Laws: Introducing PIPA | Ground Labs**
<https://www.groundlabs.com/blog/south-koreas-privacy-laws-introducing-pipa/>

8 9 10 12 14 **Security Requirements and Breach Notification | South Korea | Global Data and Cyber Handbook | Baker McKenzie Resource Hub**
<https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/south-korea/topics/security-requirements-and-breach-notification>

17 18 **Statutes & Regulations | KoFIU**
<https://kofiu.go.kr/eng/law/law.do>

19 20 **Customer Due Diligence - BNP Paribas in South Korea**
<https://www.bnpparibas.co.kr/en/customer-due-diligence/>