Legal 500
Country Comparative Guides 2025

Germany

Fintech

Contributor

SCHALAST LAW | TAX

Prof. Dr. Andreas Walter, LL.M.

Attorney-at-law (Rechtsanwalt) | Partner, Head of Banking & Finance Practice Group | andreas.walter@schalast.com

Simon Waldbröl

Attorney-at-law (Rechtsanwalt) | Partner, Banking & Finance | simon.waldbroel@schalast.com

This country-specific Q&A provides an overview of fintech laws and regulations applicable in Germany.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Germany: Fintech

1. What are the regulators for fintech companies in your jurisdiction?

In Germany, various regulatory authorities oversee FinTech companies depending on the type of activity the company engages in. The main regulatory bodies are:

The **BaFin (Federal Financial Supervisory Authority)** is the central authority responsible for overseeing financial service providers in Germany. It monitors banks, insurance companies, investment firms, and financial service providers, including FinTech companies offering financial products or services. This includes the regulation of payment services, e-money, and crowdfunding platforms. BaFin ensures that FinTech companies comply with consumer protection requirements, capital requirements, and transparency standards.

The **Deutsche Bundesbank** also plays a role in overseeing financial stability and monetary policy in Germany. While it works closely with BaFin, it influences financial market regulation, particularly when it comes to payment systems and compliance with stability-related regulations.

At the European level, the **European Central Bank (ECB)** is involved in the regulation and oversight of financial institutions, especially regarding systemic risks and the security of the euro area. This particularly includes the largest banks in Germany that are under direct supervision of ECB.

The **European Banking Authority (EBA)**, as European Union regulatory agency, sets the regulatory framework for banks, including FinTech companies. It plays a role in harmonizing regulatory requirements across the EU.

2. Do you foresee any imminent risks to the growth of the fintech market in your jurisdiction?

One of the major concerns for FinTechs probably is data security. The number of cybercrimes in Germany rises approx. 8 to 15 % each year – with an exponential increase during the Covid pandemic. The aggregated damage is estimated to exceed 100 billion Euros. The more cyberattacks become publicly known, the more likely customers lose trust in the affected sector. The prevention of cyber-attacks is therefore essential to scale digital banking products. This, in turn, leads to rising costs for this prevention. Not necessarily in conjunction with a cyber-attack but no less harmful to the market are money laundering and terror financing activities. German neobanks have been massively criticised not least by BaFin but the entire industry. Neobank services were used for money laundering and the AML prerequisites were not deemed sufficient.

In our view, the German FinTech market provides for a variety of customer onboarding and KYC tools that fully comply with legal requirements and provide a certain convenience to customers – and also effectively safeguard the interests at stake. The downside of providing most of the population with flexible payment solutions such as BNPL products could be a credit default increase. Should more and more defaults realise, yields would shrink in the short term. In the long term, we see at least a potential cluster risk should, for example, the refinancing of more and more FinTechs fail.

3. Are fintechs required to be licensed or registered to operate in your jurisdiction?

In addition to general civil law, the legal framework for FinTech structuring is shaped by regulatory provisions, for example the Banking Act and the Payment Services Supervision.

Legislators and supervisory authorities are faced with the challenge of reducing the “blind spot” as far as possible in regulatory terms. Such regulatory gray areas arise because the Banking Act differentiates between financial service providers on the one hand and banks on the other. Inasmuch as FinTechs cannot always be unequivocally qualified as one or the other, regulatory requirements are not always clearly established in advance. Triggered by new product development on the FinTech market, German authorities are faced with a constant race to uncover the associated risks and regularly adapt the legal and regulatory requirements – same as FinTechs themselves, who face the challenge of constantly adapting changes in the regulatory landscape.

As there is no specific FinTech license in Germany, the regulation of FinTech companies ultimately depends on their business activities. This is also the result of a technology-neutral “same business, same risk, same rules” approach. This means that the entire range of licenses and marketing restrictions can become relevant for FinTech business models.

However, what can be said conclusively is that many “young” FinTechs partner with established players such as fronting banks and or fronting payment service providers to use their licence in a white label solution. As soon as FinTechts have tested the market appropriately and are somewhat established, many FinTechs endeavour their own licences and opt-in to be regulated themselves.

4. What is a Regulatory Sandbox and how does it benefit fintech start-ups in your jurisdiction?

The model of a “regulatory sandbox” is an area where FinTech companies can test and develop their business models under supervision and with certain relaxations. However, BaFin rejects this model.

BaFin and the legislator currently deny the introduction of a regulatory sandbox in Germany. Sandboxes are quite popular in other jurisdictions and market participants, particularly start-ups with yet small resources, demand the introduction of such sandboxes also in Germany. Although denying such regulatory sandbox, BaFin is well aware that young players are required to breathe under all the regulatory requirements and tends to adjust the intensity of the supervision depending on the risk associated with a given business model, taking into account the principle of proportionality: While for identical risks and identical business models identical regulatory standards should apply, BaFin at the same time wants to give new players the room to grow into their regulatory status. Furthermore, BaFin establishes special divisions for concentrating specific expertise, for example in connection with the new Markets in Crypto Assets Regulation (‘MiCAR’) on an EU level and a continuously updated catalogue regarding FinTech. Furthermore, Frankfurt, Germany, will be hosting the new European Anti-Money Laundering Association (‘AMLA’).

5. How do existing securities laws apply to initial coin offerings (ICOs) and other crypto assets, and what steps can companies take to ensure compliance in your jurisdiction?

In Germany, the regulatory framework for evaluating crypto tokens is shaped by a combination of European and national laws, with BaFin (the Federal Financial Supervisory Authority) overseeing compliance. Since January 2019, the first “token securities prospectuses” have been approved. Whether a crypto token or an ICO (Initial Coin Offering) is subject to regulatory oversight is determined by BaFin on a case-by-case basis, using existing laws and a technology-neutral approach.

There are two key regulatory areas: the prospectus obligation and the licensing obligation. The prospectus obligation means that before publicly offering securities or admitting them to a regulated market, a corresponding prospectus must be created and published. This prospectus must include all essential information about the issuer and the offered securities to allow investors to make informed decisions. The prospectus obligation is governed by the Prospectus Regulation and relevant European Delegated Regulations.

The licensing obligation refers to activities that can only be conducted after obtaining permission from BaFin, as outlined in the German Banking Act (KWG) and other relevant supervisory laws. This includes both the issuance of crypto tokens and subsequent trading activities. Whether licensing is required depends on the regulatory classification of the tokens and the specific activities involved.

In summary, whether a crypto token or ICO requires a prospectus or license is determined by its specific design and nature, ensuring regulatory clarity and fair supervision.

6. What are the key anti-money laundering (AML) and Know Your Customer (KYC) requirements for cryptocurrency exchanges in your jurisdiction, and how can companies implement effective compliance programs to meet these obligations?

MiCAR (Markets in Crypto-Assets Regulation) has been the first comprehensive cryptocurrency regulation in the EU since the end of 2024. The regulation aims to improve consumer protection, provide legal certainty, strengthen financial stability, and promote innovation. Crypto service providers now require an EU license, and transfers in excess of EUR 1,000 between private wallets and exchanges need additional documentation. Stablecoins like USDT could face restrictions, while Bitcoin mining remains unregulated. Private wallet-to-wallet transfers are exempt from the new rules. The regulation also introduces strict security standards for crypto exchanges, ensuring they securely store assets. MiCAR establishes a unified framework across the EU, offering clearer rules for both crypto businesses and investors.

The Cryptocurrency Transfer Regulation

(KryptoWTransferV) focuses on combating money laundering and terrorism financing. Platforms facilitating crypto transfers must store customer data, including sender and recipient addresses, and monitor transactions for suspicious activity, reporting any concerns to authorities. Investors must undergo KYC (Know Your Customer) procedures to verify their identity and other personal information.

7. How do government regulations requiring licensing or regulatory oversight impact the operations of cryptocurrency and blockchain companies in your jurisdiction, and what strategies can be employed to navigate these varying requirements?

In Germany, government regulations that require licensing or regulatory oversight have a significant impact on the business activities of cryptocurrency and blockchain companies. These companies must ensure that they meet the relevant regulatory requirements in order to offer their services in compliance with applicable laws and at the same time gain the trust of customers and regulators. The most important regulatory requirements in Germany relate in particular to the Payment Services Supervision Act (ZAG), the Securities Institutions Act (WpIG) and the Money Laundering Act (GwG).

Cryptocurrency and blockchain companies offering payment services or financial services (e.g., cryptocurrency trading, issuing e-money, or providing wallet services) require a license from BaFin (the Federal Financial Supervisory Authority). Without a license, they are not entitled to legally offer their services. This licensing requirement mandates compliance with strict standards, such as ensuring financial stability, adhering to AML/KYC regulations, and safeguarding customer funds.

Under BaFin's supervision, companies must regularly report and ensure that their operations are transparent. They shall ensure that their systems and processes meet regulatory requirements, which adds compliance and reporting costs.

The regulation of blockchain and cryptocurrency companies in Germany is still evolving, which can lead to uncertainties. While some business models are already clearly regulated, there are gray areas for newer technologies or business models that are not explicitly covered by existing laws yet. This may lead to legal challenges and require companies to continuously adapt to changing regulatory requirements.

To meet AML/KYC requirements, companies should develop and implement comprehensive compliance programs. This includes setting up robust transaction monitoring systems, employee training on regulatory issues, and establishing effective procedures for customer identification and verification.

8. What measures should cryptocurrency companies take to comply with the governmental guidelines on tax reporting and obligations related to digital assets in your jurisdiction?

In Germany, cryptocurrency companies are required to particularly comply with income tax, value-added tax (VAT), and trade tax obligations. These tax obligations arise from the Income Tax Act (EStG), the Value Added Tax Act (UStG), as well as specific regulations issued by the Federal Ministry of Finance (BMF) and tax authorities. However, these tax obligations are not specifically addressing cryptocurrency companies.

Profits from the sale or exchange of cryptocurrencies must be taxed. This applies to both businesses and individuals engaged in significant cryptocurrency trading. Specifically, profits from trading cryptocurrencies may be taxable as income from business operations or private sales.

In Germany, cryptocurrency trading is generally exempt from VAT when used as a means of payment. However, specific services such as token issuance or providing payment services may be subject to VAT.

Cryptocurrency companies engaged in business activities, such as trading or offering mining services, are generally subject to trade tax. These companies must account for trade tax obligations in their financial operations.

Cryptocurrency companies are required to report all relevant income from digital assets in their tax returns. This includes income from brokering or trading crypto assets, which must be properly reflected in the income tax return and, if applicable, in the VAT return.

If a cryptocurrency company operates internationally, it must also ensure compliance with the tax regulations of the respective countries in which it operates. Many countries, including EU member states, have specific rules for dealing with cryptocurrencies, and it is essential to adhere to these international standards to avoid tax issues and double taxation.

9. How can blockchain companies address data privacy and protection regulations in your jurisdiction, while ensuring transparency and security on decentralized networks?

The MiCAR and DSGVO (General Data Protection Regulation (GDPR)) in particular serve to ensure compliance with data protection and data security as well as transparency.

The MiCAR (Markets in Crypto-Assets Regulation) is applicable since 30 December 2024, with the exception of the provisions regarding stablecoins, which is in effect since 30 June 2024. MiCAR includes regulations for the primary market, i.e., the issuance and trading approval of crypto assets, as well as the secondary market concerning crypto asset services. The overarching goal of MiCAR is to ensure user trust in crypto markets and to maintain market integrity. MiCAR specifically includes provisions on the supervision of crypto asset service providers, transparency and disclosure requirements related to public offerings and trading approval of crypto assets, as well as rules to combat market abuse.

GDPR applies to the processing of personal data, and blockchain companies must ensure that any personal data processed or stored on their networks complies with its principles. While decentralized networks may inherently make it challenging to identify a “data controller” or “data processor,” companies must still adhere to the GDPR requirements when dealing with personal data, such as ensuring data protection by design and by default.

Blockchain companies should avoid storing personally identifiable information (PII) directly on the blockchain. If personal data is necessary for certain blockchain operations (such as in smart contracts), companies should ensure it is minimal, anonymized, or pseudonymized, reducing the risk of breaching data privacy laws.

Blockchain companies must implement Privacy by Design and Privacy by Default principles as required by the GDPR. This means that privacy should be integrated into the development of blockchain systems from the outset, and only the necessary data should be processed or made available by default.

In order to comply with data protection regulations, blockchain companies may use state-of-the-art technology on data anonymization and/ or data pseudonymization. Furthermore, new data trustee structures are emerging on the European market promising compliance with data protection laws for all participants. In doing so, companies can mitigate risks related to the exposure of personal data, while still benefiting from the transparency and immutability of blockchain technology.

10. How do immigration policies, such as the U.S.'s H-1B and L-1 visas, impact the ability of fintech companies to hire international talent in your jurisdiction?

Since Germany is part of the EU, access is given to the EU-wide employee market. Same applies to EEA countries. Regarding third countries, however, the flexibility depends on respective visa requirements. In practice, however, there is still some room for improvement regarding the accessibility and transparency for international talents to enter the German market, i.e. obtain a working permit. Many important institutions are located in Germany, e.g. the European Central Bank (ECB) and the European Systemic Risk Board (ESRB) or the European Insurance and Occupational Pensions Authority (EIOPA) in Frankfurt, many expatriates are being attracted to work in Germany. Furthermore, the corona pandemic possibly has helped to cover distances. Both employees and employers offer and use more often remote working solutions. It can in our view be expected that restrictions free employee movement will further reduce in the future.

Specialist shortage is a well-known problem in Germany and the legislator is concerned about improving the immigration efforts for specialists. In March 2020, the German Skilled Immigration Act (Fachkräfteeinwanderungsgesetz, ‘FachKrEG’) came into force to tackle this exact issue. This regulation aims to the migration of non-EU specialists. According to the Federal Ministry of Economics and Technology (Bundesministerium für Wirtschaft und Klimaschutz, ‘BMWK’), Germany issued approx. 30.000 visa on the basis of the said regulation in the year of the Covid pandemic 2020 which was the first year after coming into force. Furthermore, the German legislator has amended the FachKrEG for the further development of skilled labor immigration on an ongoing basis to further win skilled labor immigrants for the German market.

11. What are the key regulatory and compliance requirements that a fintech must address when entering the market in your jurisdiction, and how can the company ensure adherence to all

applicable laws and regulations?

Anyone in Germany who intends to provide certain banking and financial services requires permission from the financial regulatory authority. When determining which permission is required, the planned business model, as well as the legal and practical design of the planned products and services, are decisive.

As mentioned above, activities that require authorization include banking activities according to Section 1 para 1 of the German Banking Act (KWG), financial services transactions under Section 1 para 1a of the KWG, securities services according to Section 2 para 2 of the Securities Trading Act (WpIG), payment services according to Section 1 para 2 of the Payment Services Supervision Act (ZAG), or electronic money business under Section 1a para 2 of the ZAG, as well as any future similar activities under the MiCAR regulation.

Pursuant to Section 32 para 1 sentence 1 of the German Banking Act (KWG), anyone wishing to conduct banking business or provide financial services in Germany on a commercial basis or to an extent that requires a commercially organized business operation requires written permission from the Federal Financial Supervisory Authority. The legal form of the company (natural person, partnership, legal entity) is irrelevant.

Whether a business model requires a permit, and if so, what type of permit is required and what scope the permit must have, is to be determined on the basis of the individual circumstances in each specific case.

12. How should a fintech approach market entry strategy in your jurisdiction, considering factors such as target customer demographics, competitive landscape, and potential partnerships with banking and other financial institutions?

To develop a successful market entry strategy, a FinTech startup should proceed systematically. First, it must conduct a thorough analysis of the target customer demographics. This includes examining the age structure, technical affinities, and financial needs of potential customers. For example, a mobile payment app might appeal to a younger audience, while a platform for digital wealth management would be more suitable for affluent clients or professional investors. A clear definition of the target audience helps in selecting the appropriate channels (such as social media platforms or specific marketing channels) and developing tailored products or services that meet the specific needs of the customers.

Regarding the competitive landscape, the FinTech startup should conduct a detailed market analysis to identify existing competitors, their strengths and weaknesses, and their offerings. This allows for clear positioning, where the FinTech startup can highlight differentiation opportunities – whether through innovative features, better customer service, or more favorable terms. It is also crucial to understand the regulatory requirements and challenges of the market to avoid legal pitfalls and gain customer acceptance.

Additionally, the FinTech should actively seek partnerships with established banks and other financial institutions. These partnerships offer several advantages, such as access to established customer networks, trust, and resources. One option could be integrating FinTech products into existing banking services, for example, through APIs or collaboration agreements that allow customers to seamlessly combine FinTech solutions with traditional banking services. Furthermore, partnerships with established financial institutions can help overcome regulatory hurdles and accelerate the introduction of new products.

In summary, and particularly for international FinTechs, it might make sense to enter the EU market by testing the largest market by headcount that, in addition to this, is known for its supervisory authorities being rather strict but is assigned a kind of quality sign. Therefore, for many FinTechs from overseas, Germany is an important go-to market.

13. What are the primary financial and operational risks associated with entering the market in your jurisdiction, and how can the fintech effectively mitigate these risks to ensure a smooth transition and sustainable growth?

In entering a new market, FinTechs face various financial and operational risks. In addition to these, regulatory risks arise in connection with their business model due to strict compliance with laws such as the KWG, WpIG, and ZAG. Performing a regulated business requires – not only in Germany – constant monitoring and legal support.

To face the intense market competition on the German market, FinTechs need a unique selling point (USP). This is supported by the regulator's view that Germany is overbanked anyway, particularly given their legacy savings banks system.

With the current global tension, also economic risks on a national level, such as a recession, cannot be excluded.

14. Does your jurisdiction allow certain business functions to be outsourced to an offshore location?

Financial sector companies are increasingly outsourcing services to specialized providers. This offers many advantages. However, outsourcing also makes the financial market more vulnerable. Therefore, it must be reported to the financial supervisory authority, BaFin. The BaFin has guidelines that the addressees must follow. The requirements for outsourcing agreements are rather strict and – most importantly – the regulated entity on the ground in Germany remains fully obliged and responsible for regulatory law compliance.

15. What strategies can fintech companies use to effectively protect their proprietary algorithms and software in your jurisdiction, and how does patent eligibility apply to fintech innovations?

In Germany, FinTech companies can protect their proprietary algorithms and software through several legal strategies such as trade secrets under the German Trade Secrets Act by keeping the information confidential with internal security measures and non-disclosure agreements (NDAs). However, given that there is a residual risk of NDAs being breached, FinTechs may consider copyright and patent protection.

Software code is automatically protected by copyright under the German Copyright Act. It shall be noted, however, that this copyright protection solely covers the expression of code, not the underlying ideas.

Innovations that involve technical solutions to problems, such as novel algorithms integrated into technical systems like blockchain, are best protected by patents. However, purely abstract business models or algorithms without a technical effect are generally not eligible for patent protection.

Additionally, FinTech firms can use licensing agreements to control how their software is used, and blockchain technology can provide inherent protection through decentralization and transparency.

16. How can a fintech company safeguard its trademarks and service marks to protect its brand identity in your jurisdiction?

In Germany, a FinTech company can protect its trademarks and service marks by registering them with the German Patent and Trademark Office (DPMA). The registration grants the company exclusive rights to use the mark in connection with specific goods or services. For broader protection across Europe, and depending on its target markets, the company can also register the trademark with the European Union Intellectual Property Office (EUIPO).

To safeguard its brand identity, the company should regularly monitor for trademark infringements and take legal action, such as sending cease-and-desist letters if necessary. Additional protective measures include registering variations of the mark and ensuring timely renewal of the trademark every ten years. The German Trademark Act (Markengesetz) provides the legal framework for trademark protection in Germany.

17. What are the legal implications of using open-source software in fintech products in your jurisdiction, and how can companies ensure compliance with open-source licensing agreements?

If FinTechs are financial entities within the meaning of REGULATION (EU) 2022/2554 ("**DORA**"), they must set up an ICT risk management framework. This shall include, at a minimum, policies, guidelines, procedures, ICT protocols and tools necessary to properly and adequately protect all information and ICT assets, including computer software, hardware and servers, and to protect all relevant physical components and infrastructure, such as premises, data centers and designated sensitive areas, to ensure the adequate protection of all information and ICT assets from risks, including damage and unauthorized access or use. In the case of open source software, care must therefore be taken to ensure that it is used within the risk management framework and does not pose any risks. In case they are ICT third-party service providers, they have to make sure they comply with the agreement concluded with the financial entity, also with regard to the usage of open-source software.

18. How can fintech startups navigate the complexities of intellectual property ownership when collaborating with third-party developers or entering into partnerships?

Trademark protection prohibits competitors to use the same (or confusingly similar) corporate design, such as brand names and logos or layouts. Patent protection prohibits competitors to copy inventions. Since patent protection is more relevant to manufacturing and production industry, trademark protection is recommended to consider for FinTechs.

The German Copyright Act (Urheberrechtsgesetz, 'UrhG') protects IP in a narrow sense. For FinTechs, protecting source codes and app interfaces but also texts, audios, videos, pictures etc. could be of interest. Other than trademarks, IP protected under the UrhG cannot be transferred or assigned whatsoever and always remain with the originator.

However, the use of IP rights under the UrhG by third parties can be contractually agreed on.

19. What steps should fintech companies take to prevent and address potential IP infringements, such as unauthorized use of their technology or brand by competitors?

From the perspective of German law, FinTech companies should take several steps to prevent and address potential infringements of their intellectual property (IP) rights, such as unauthorized use of their technology or brand by competitors. First, they should register their IP rights, including trademarks, patents, copyrights, and trade secrets, with the German Patent and Trademark Office (DPMA) or other relevant international authorities to ensure legal protection. This provides clear documentation and enforceability of rights in case of infringement.

Additionally, it is important to regularly monitor the market and competitors to identify potential IP violations. This can be done through trademark watch services or patent and trademark searches. If an infringement is detected, FinTech companies should respond quickly by sending a cease-and-desist letter to the competitor or, if necessary, initiate legal actions such as an injunction or damages claim.

To protect their technology and trade secrets, FinTechs should use non-disclosure agreements (NDAs) when working with third parties. These agreements provide legal protection against unauthorized use or disclosure of confidential information. Furthermore, it is advisable to regularly train employees on IP protection and confidentiality, and to include clear provisions in employment contracts that address the assignment of invention rights and confidentiality obligations.

Finally, clear contractual agreements should be made when collaborating with external partners or service providers to govern the use and protection of IP. Overall, these measures allow FinTech companies to effectively protect and enforce their intellectual property rights under German law.

20. What are the legal obligations of fintechs regarding the transparency and fairness of AI algorithms, especially in credit scoring and lending decisions? How can companies demonstrate that their AI systems do not result in biased or discriminatory outcomes?

Under the new EU AI Regulation, FinTech companies have specific legal obligations to ensure the transparency and fairness of their AI algorithms, particularly in areas like credit scoring and lending decisions. They must ensure that their AI systems are transparent, meaning that the decisions made by the algorithms can be explained and understood by both users and regulators. Companies must also take steps to ensure that their algorithms do not result in biased or discriminatory outcomes, which includes regular assessments to identify and mitigate any potential bias.

To demonstrate fairness and non-discrimination, FinTechs should implement mechanisms for auditing and monitoring AI systems, provide clear explanations of the decision-making process, and conduct impact assessments to evaluate how their AI models affect different demographic groups. They must also ensure that any training data used does not contain discriminatory biases and that the AI system adheres to both legal and ethical standards. Regular testing and documentation of these measures can further support compliance with the new AI regulation.

21. What are the IP considerations for fintech companies developing proprietary AI models? How can they protect their AI technologies and data sets from infringement, and what are the implications of using third-party AI tools?

FinTechs must comply with REGULATION (EU) 2024/1689 ("**AI-Act**") laying down harmonised rules on artificial intelligence. Extensive information with regard to the AI-Act can be found on the website of the European Commission.

22. What specific financial regulations must fintechs adhere to when deploying AI solutions,

and how can they ensure their AI applications comply with existing financial laws and regulations? Are there specific frameworks or guidelines provided by financial regulatory bodies regarding AI?

The most important financial regulations are REGULATION (EU) 2022/2554 ("**DORA**") on digital operational resilience for the financial sector and REGULATION (EU) 2024/1689 ("**AI-Act**") laying down harmonised rules on artificial intelligence. In order to comply with these regulations they need external legal advice or internal legal expertise. Extensive information on DORA can be found on the website of the German Federal Financial Supervisory Authority and on the website of the European Banking Authority and with regard to the AI-Act on the website of the European Commission.

23. What risk management strategies should fintech companies adopt to mitigate potential legal liabilities associated with AI technologies?

FinTechs should firstly classify their AI systems into risk categories, as required under the EU AI Act. They should furthermore ensure that high-risk applications, such as AI-based credit scoring or fraud prevention, meet stricter requirements.

Secondly, FinTechs must ensure their AI systems are compliant with data protection laws and conduct regular audits to ensure ongoing legal compliance. Ethical use and avoidance of biases are also key requirements.

Any remaining liability risks should be mitigated by concluding state-of-the-art legal contracts, insurance, and regular staff training on the AI Regulation.

24. Are there any strong examples of disruption through fintech in your jurisdiction?

Fintechs disrupt the traditional banking system by addressing its major weaknesses. While traditional banks face delays in transactions, limited working hours, low interest rates, and lack of flexibility, FinTechs provide faster, more flexible, and cost-effective solutions. Fintech companies enable real-time transactions, offer 24/7 access, and create innovative financial products like peer-to-peer lending and decentralized finance (DeFi) solutions. Additionally, FinTechs use technologies like blockchain, AI, and machine learning to offer more efficient and transparent financial products. These developments, combined with the pandemic and the smartphone revolution, have led to a market shift, with banks increasingly losing market share to FinTechs and being forced to modernize their core banking systems.

25. Which areas of fintech are attracting investment in your jurisdiction, and at what level (Series A, Series B, etc.)?

Currently, RegTech (e.g. Finom, AuditOne), ComplianceTech (e.g. pliant, sinpex) and digital assets companies (e.g. bunch, Timeless) seem to be most attractive to large scale investments.

The German market has gone through a serious consolidation phase with many FinTechs emerging from start-up to grown-up. This leads to funding rounds in all of the categories from seed through Series C. It is rumored that the pipeline for German FinTech IPOs is full, with the most prominent IPO rumor of 2024 being Raisin, formerly Weltsparen.

Contributors

Prof. Dr. Andreas Walter, LL.M.
Attorney-at-law (Rechtsanwalt) | Partner, Head of Banking & Finance Practice Group
andreas.walter@schalast.com

Simon Waldbröl
Attorney-at-law (Rechtsanwalt) | Partner, Banking & Finance
simon.waldbroel@schalast.com