Cryptocustody businesses in Germany

BaFin publishes guidance on the application procedure

Since 1 January 2020, providers of 'cryptocustody business' (i.e. the safekeeping, administration and safeguarding of crypto-assets or private cryptographic keys that serve to hold, store or transfer crypto-assets) in Germany are required to hold a license as a financial services institution under the German Banking Act (*Kreditwesengesetz,* 'KWG') (please refer to our Client Briefing of 4 March 2020, available here, for further detail on the scope of the regulated business).

This licence requirement has been introduced into German law in the course of the transposition of the fifth anti-money laundering directive (Directive (EU) 2018/843 or '5AMLD'), but significantly goes beyond the original scope of the directive, in particular as 5AMLD only requires the registration of cryptocustody providers. Thus, there is currently no European framework or guidance that establishes the initial and ongoing requirements for licensed providers of cryptocustody business.

For this reason, on 1 April 2020, BaFin published long-awaited 'Guidelines on applications for authorisation for cryptocustody business' (in English and German) (the 'Guidelines'), in which it describes the requirements that it considers to be particularly important when applying for a licence for cryptocustody business. The Guidelines focus on IT security requirements and the qualification of managing directors (*Geschäftsleiter*). This briefing summarises the main aspects of the Guidelines.

General remarks on the application procedure

Providers of cryptocustody business that wish to apply for and receive a licence under the KWG generally need to file an application with BaFin and the German Central Bank (*Deutsche Bundesbank*) pursuant to section 32 KWG. The documents and information that must be submitted are set out in section 14 of the German Regulation on Notifications under the KWG (*Anzeigenverordnung*, 'AnzV'). Further relevant guidance is published in the 'Guidelines on the granting of authorisation to provide financial services of 6 July 2018' by Deutsche Bundesbank. The procedure is subject to a fee (which amounts to EUR 10,750 in case of a licence application limited to the provision of cryptocustody business).

New providers of cryptocustody business need to assess whether their intended business model also triggers licence requirements for other regulated activities. For instance, should some of the crypto-assets taken into custody qualify as securities pursuant to the German Custody Act (*Depotgesetz*, 'DepotG'), the provider may require a (securities) custody business license (i.e. a banking license) in addition to the licence for cryptocustody business (please refer to our Client Briefing of 4 March 2020, available here, for further detail).

BaFin further states, that, should crypto-assets also qualify as financial instruments pursuant to Section C of Annex of Directive 2014/65/EU ('MiFID II'), additional licences may be required for other banking activities or financial services. The qualification of crypto-assets as MiFID financial instruments appears, however, not relevant for the question of whether (additional) licence requirements are triggered for the service provider. The definition of financial instruments under the KWG is considerably broader than the MiFID definition. For instance, offering trading activities covered by MiFID with regard to crypto-assets generally requires a separate licence (e.g. for providing principal broking services (*Finanzkommissionsgeschäft*), contract broking (*Abschlussvermittlung*) or trading on own account (*Eigenhandel*) irrespective of whether the crypto-assets in question qualify as MiFID financial instruments (e.g. virtual currencies). In these cases, the qualification of crypto-assets as financial instruments within in the meaning of the German Securities Trading Act (*Wertpapierhandelsgesetz*, 'WpHG') may trigger additional governance and conduct requirements for the service provider.

Should businesses – as a result of the type of regulated activities they provide – qualify as MiFID investment firms, the application procedure is subject to the requirements of Regulation (EU) 2017/1943 and Regulation (EU) 2017/1945.

Specific requirements for the application of providers of cryptocustody business

IT security requirements

As other licensed financial service providers, cryptocustody business providers must have a proper business organisation, which ensures compliance with applicable law and operational needs (section 25a KWG). For cryptocustody business, IT security forms an important part of the proper business organisation that needs to be demonstrated in connection with the internal control system in the licence application. The relevant requirements are set out in more detail in the Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement,* 'MaRisk') and the Supervisory Requirements for IT in Financial Institutions (*Bankaufsichtliche Anforderungen an die IT*, 'BAIT") and also need to be taken account when establishing the risk management system for providers of cryptocustody business.

According to the Guidelines, BaFin expects to receive detailed information on the firm's IT security strategy, the handling of security incidents and a risk assessment and the existing technical and organisational methods for the use of cryptographic keys in the course of the licensing procedure.

In this context, details of the business model from a technical perspective must also be provided, including a description of how crypto-assets are technically held, i.e. which form of storage is used (e.g. 'hot wallet' or 'cold wallet'), and whether and how crypto-assets are held in custody for individual customers in separate or pooled wallets.

On the basis of the business model, the IT systems have to be described comprehensively. According to the Guidelines, the information must in particular comprise:

- a detailed description of the business strategy in relation to the planned activity;
- the IT strategy according to the requirements of AT 4.2. MaRisk (in particular a sustainable business strategy defined by the managing directors). The requirements for IT strategies are also set out in para 1. BAIT;
- a detailed description of the IT system architecture (in particular a description of the network and backup elements, but also specific hardware used for the safekeeping of crypto-assets);
- a description of the IT security strategy (including an explanation of the technical and organisational security measures that were implemented, as well as relevant encryption methods);
- information on (material) outsourcings and cloud solutions used (including information on all cooperation partners and their roles) and on fulfilment of the requirements set out by AT 9 MaRisk and BaFin's 'Guidance on outsourcing to cloud service providers';
- a risk assessment and an explanation of the impact of relevant risks (e.g. the loss of cryptographic keys but also of other key data and IT infrastructure) and the measures taken to address them;
- a detailed description of the relevant 'crypto concept' (including a description of the cryptographic functions and methods used in IT technical terms)
- information on the contingency management and measures that have been implemented to prevent a loss of the crypto-assets held in custody;
- information on the role-based security concept or user access management (cf. para 5 BAIT) after having identified the roles with access to sensitive data and cryptographic keys held in custody; and
- a description of the monitoring procedures that have been implemented (e.g. the system monitoring process).

Requirement to appoint reliable and qualified managing directors

Section 25c (1) KWG requires managing directors of financial service providers to be fit and proper. In particular, they need to have sufficient theoretical and practical knowledge and expertise in the relevant areas of business, as well as management experience.

Should managing directors have three years of management experience in a (regulated) institution of a similar size and business model, they can benefit from the presumption that they are sufficiently qualified. However, fulfilling the prerequisites of this presumption may be difficult, given that the regulated activity of cryptocustody business is based on relatively new technology and has been largely unregulated so far. Against that background, qualifications will, at least for now, need to be assessed in each individual case.

BaFin has previously issued a 'Guidance notice concerning managing directors pursuant to the KWG, the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz, – ZAG) and the German Investment Code (Kapitalanlagegesetzbuch – KAGB)' in order to provide further guidance on its interpretation of these requirements. The principles set out therein are generally applicable also in the context of cryptocustody business. However, BaFin emphasizes three points specifically in relation to cryptocustody business where it deviates from that guidance.

- BaFin will limit its assessment of the required **theoretical and practical expertise** to the 'technical expertise' of the managing directors, arguing that 'cryptocustody business is essentially based upon technical processes and the security of the cryptographic keys held in custody is particularly important'. Thus, should managing directors be able to demonstrate their 'technical expertise' by relevant academic credentials and by 'extensive practical experience in IT security', this would be considered expertise '**in the**

relevant areas of business'. A similar interpretation has been made in relation to the management board's IT expertise for other banking businesses – to which BaFin explicitly refers.

- In relation to **practical expertise**, BaFin will particularly consider as 'practical experience' those activities 'which have an appropriately elevated hierarchical status' within undertakings that fall under the scope of the transitional regime for cryptocustody business (section 64y KWG). This may, depending on the size of the undertaking, not only include managing directors, but also the level directly reporting to them. Similar to BaFin's administrative practice for management board's IT expertise for other banking businesses, BaFin expects that managing directors use the time in which firms operate under the temporary regime 'to further develop areas of expertise which they have not yet completely mastered'. BaFin might therefore expect managing directors to attend trainings on, for example, ongoing prudential regulation or AML requirements until the licence is granted.
- BaFin may also accept **a lesser degree of expertise** by one of several managing directors in individual cases, should 'the human resources and organisational structure of the undertaking' be suitable to temporarily compensate for that lack of knowledge.

Minimum number of managing directors

If cryptocustody business is the only regulated service that is provided, only one managing director is generally required by law. However, pursuant to BaFin, more than one managing director may be necessary where the requirements of having in place a proper business organisation would otherwise not be fulfilled considering the size of the institution and its business activities.

Anti-money laundering and counter-terrorist financing requirements

Financial services institutions are subject to rules relating to the prevention of money laundering and terrorist financing that are mainly set out in the German Anti Money Laundering Act (*Geldwäschegesetz*, 'GwG'). These requirements already apply to providers of cryptocustody business that carry out their business on basis of the temporary regime. However, BaFin states that it will apply the sanctioning regime for violations of these rules in a proportionate manner for AML measures whose establishment may require some time for becoming operational in individual cases. BaFin further announces that it will publish additional guidance in relation to the AML requirements that cryptocustody businesses must comply with.

Application for a license while using the temporary regime

The legislator has granted cryptocustody providers that started to provide their services in Germany before 1 January 2020 a temporary permission to continue to provide their services subject to (i) their notification of intent to submit an application for a licence by 31 March 2020 and (ii) the submission of a complete licence application by 30 November 2020 (section 64y KWG). The transitional regime applies until BaFin's decision on the licence application (please refer to our Client Briefing of 4 March 2020, available here, for further detail).

The BaFin Guidelines explain that providers using the temporary regime are already considered 'institutions' pursuant to the KWG and that the (ongoing) requirements of the KWG already apply to them. BaFin therefore expects them to undertake adequate efforts to comply with the legal requirements in a timely manner. BaFin states that it would refuse to grant the licence in cases where the providers have not adapted their processes during the transition period granted by the legislator. BaFin further expects, that, should providers not comply with certain requirements at the time they file their application, they should be able to explain (i) the underlying reasons (ii) a schedule for the timely implementation and (iii) an assessment of the technical risks expected during the time until implementation and counter measures during that period.

For more information, please contact one of the team:

Markus Benzing
Partner
T +49 69 27308 276
E markus.benzing@freshfields.com

Alexander Glos
Partner
T +49 69 27308 191
E alexander.glos@freshfields.com

Daniel Klingenbrunn
Associate
T +49 69 27308 726
E daniel.klingenbrunn@freshfields.com

Heinrich Nemeczek
Associate
T +49 69 27308 147
E heinrich.nemeczek@freshfields.com

freshfields.com