Appendix to BaFin's response

Explanation to question 27:

Supplementing the assessments above (Other): facilitating access to the data stated also appears sensible from the consumer's point of view, since this would expedite the proposal examined by the Commission within the scope of the European Financial Transparency Gateway Project (EFTG) about creating a single point of access to information relevant for investors in listed European companies.

Explanation to question 28

Explanation of the selection made

- A basic requirement that should be fulfilled in advance is the single definition of data in the sense of a data dictionary.

- Standardisation (regarding format), harmonisation and interoperability (particularly in order to access, exchange, integrate and cooperatively use data in a coordinated manner) enable automation, cost-efficiency and scalability of use cases and are therefore necessary for easy EU-wide use of data.

- Regarding „public data base": The mere indication that databases should be public is not sufficient for an assessment. Among other things, the type of data to be made available, the authorization concept and the governance model are essential for a sound evaluation. That is why we have chosen the tick box "N.A.".Explanation to question 30

Explanation to question 30

Explanation of the selection made

- Depending on the specific design of the open finance policy, consumers could potentially be offered services that are more innovative, more convenient and/or more appropriate to their specific situation. Whether this then results in lower prices also depends on whether open finance leads to efficiency increases on the part of the undertakings and whether the undertakings pass these on to consumers. However, open finance does not by itself prevent the emergence of market dominant positions which ultimately have a detrimental impact on consumers (for further remarks on level playing field issues see questions 31, 32 and 34).

- Open finance can constitute the basis for new business models that can be implemented by both new as well as established undertakings, either alone or in cooperation.

- Open finance can facilitate access to additional and larger data records which, in turn, are the basis for the application of technologies, particularly in the area of artificial intelligence. However, this does not necessarily require personal data, but may also use anonymised data.

- Whether and how retail investors and/or small enterprises would benefit through open finance from improved access to the capital markets and to loans crucially depends on the products in question and the design of the open finance. For instance, an automated flow of transaction data could – with the SME's consent – also accelerate the granting of credits and increase competition between credit institutions. To this extent, neither of these two questions can be answered without further details being specified. Other segments could also be mentioned in addition to these two segments (e.g. access to consumer loans and real estate financing, access to insurance products) where access for consumers could also be influenced by open finance; this is not an exhaustive list of financial segments that could be influenced by open finance. However, next to these potential benefits one also has to consider the risks associated with open finance; risks and benefits need to be weighed before any concrete open finance arrangement is put in place. In particular, when new players enter the market the emergence of regulatory arbitrage must be prevented (see also the next questions for further considerations on establishing a level playing field).

- In terms of the design of open finance policy, there is a need to consider both the interests of the financial undertakings that have verified, structured, standardised and "refined" customer data at high financial cost, as well as the interests of the companies interested in using the data and in particular the interests of customers. In this context, an assessment is

needed of whether the approach familiar from PSD2 regarding the free data usage by third parties should also be maintained in the event of extensions within the meaning of open finance. In particular, a regulation on compensation may promote a level playing field in those situations where it is not just raw data that is being transmitted, but also information gained or validated from an undertaking's own internal analyses under additional costs. A regulation on compensation also provides a greater incentive to provide premium-quality access interfaces, and this then makes it less likely that the costs for the interfaces will be passed on to end customers in the form of higher prices. However, this then also gives rise to the risk that financial undertakings will attempt to block access by inflating charges.

Explanation to question 31

Explanation of the selection made

- Data protection and the protection of privacy are fundamental prerequisites for the success of open finance, particularly when it comes to sensitive financial data.

- Financial exclusion could affect those customers who do not consent to a data transfer (open finance). The risk of financial exclusion could force customers to consent to the data transfer even though the customer does not really want this. This should not be confused with a consumer's obligation to provide the data required by law for the conclusion of a contract (e.g. data used to assess the risk in the case of loans or insurance policies); this obligation continues to apply.

- There is a risk of improper use of the access to data, not only for the purposes of optimising prices, but also within the scope of alternative use that the customer does not want or has not consented to, e.g. where financial data is used and/or combined with other data in order to personalise additional offers not related to finance.

- The relevance essentially depends on the design of the open finance policy. Data alone, such as transaction data for payment transactions, do not, at first, reveal any proprietary information as in the context of an in-house analysis/assessment. However, this could be different in the case of information/knowledge about customers that is generated by the undertaking on the basis of data, e.g. risk scoring for loans, property/collateral valuations for loans or risk assessments for insurance policies.

- Increased cyber risk: Opening new interfaces also always enables new opportunities for attack; however, the regulation of existing open finance offers that have been unregulated up until now provides the opportunity for new security standards to be enforced.

- This could result in an unlevel playing field, depending on the specific design of the open finance. It is important, therefore, to ensure that there is a level playing field both in terms of exchanging data, i.e. who is able to access what data (information) at what costs, as well as in terms of supervising the undertakings. Above all, the principle of the PSD2 should be adhered to here, i.e. that financial data may only be used by regulated providers and with the customer's consent, possibly in return for a fee reflecting that both data and data quality are assets – a fact that is aptly demonstrated by the worth of data-driven tech companies. The objective must be to ensure fair competition between traditional supervised undertakings, which have less experience with data-driven business models, and enterprises which are supervised but embedded in a larger integrated, technology-based and cross-sectoral platform concept. The latter can combine their data with a multitude of additional data sources that financial sector participants have no free access to, such as massive e-commerce platforms and sensor data from mobile operating systems. This means that the added value that can be drawn derived from payment data is vastly different and could lead to even more concentration in the hands of non-European tech and platform enterprises. Hence, it must be ensured that there is no regulatory arbitrage and no negative impact on competition that would offset the advantages of open finance. For further considerations concerning how to keep up/establish a level playing field between traditional supervised undertakings and new market players please also see the answers to questions 32 and 34.

Explanation to question 33

It is not possible to provide a blanket assessment of the benefits of open finance, and any assessment should instead be based on individual products/sectors in the financial industry; open finance should not be an end in itself. It seems sensible therefore to start, at a higher level, by dealing with specific products and their necessary data, and the benefits of an exchange of data. There should also be some clarification here regarding the data that should now be part of open finance, and the data that should not be (data, information, knowledge, proprietary information). We should then also consider whether open finance is really able to deliver more innovations, improved offerings and more convenience. Finally, if open finance is

to actually work out, consumers and/or owners of the data must also see a benefit to consenting.

Explanation of the selection made

- In the case of deposit products, open finance could lead to comparison portals, which partially also arrange deposits with institutions in other European countries, being able to present offers to customers in a more proactive way. However, the benefits of this data transfer are rather modest when compared with the input/provision by consumers.

- Open finance is relevant primarily in the area of private loans. The payment transaction data that can be accessed via the PSD2 can already be used also for financial offers today. This applies in principle to consumer loans, but can also apply to private real estate financing. The outcome of property/collateral valuation would also be of interest in private real estate financing. Whether this can be part of an exchange of data, and whether this would potentially bear a charge, is questionable. The same applies to the risk score.

- The benefits of open finance are also possible in principle with SME financing. However, since SME financing can affect various products (credit line, loans, leasing, etc.) and therefore other data may in turn be required, no statement can be made here, as there is also a question regarding which data should now form part of open finance.

- In the area of investment products for retail investors, open finance could further simplify deposit transfers and hence have a beneficial effect.

- Sales of insurance products in all segments can also benefit from open banking as a sub-category of open finance, for instance by being able to determine the need for insurance cover for banking customers based on their account transfers and payment flows, whether in terms of new insurance policies or in designing optimisation requirements.

- The benefits essentially depend on the specific product when it comes to the insurance industry itself. In the area of indemnity/accident insurance, data transfer could be useful in those insurance lines where the policyholder is required to provide much information prior to the contract

due to a higher number of tariff criteria (e.g. vehicle insurance, comprehensive residential buildings insurance). With life and hazard insurance or private health insurance, on the other hand, the question arises as to what a different provider could actually do with the data from the existing insurance, as switching to a different provider does not generally make economic sense, or a new risk assessment is required. This would also result in higher premiums, even when using open insurance, due to an increase in age when switching providers, possibly due to pre-existing conditions associated with it, and as a result of acquisition and selling expenses. The picture is similar in the case of private pension provision when life insurance is involved.

- Access to data from other sectors, such as telematics, wearables or Industry 4.0 data, benefits supervised undertakings and their customers. This is because financial undertakings are able to offer innovative, event-driven and usage-oriented products (see response to Question 34).

Explanation to question 35

Explanation of the selection made

- More attention should be paid in future open finance projects to an early, mandatory clarification of the data to be provided and of the access modality (authentication, access frequency, etc.). This does not rule out the fact that corresponding technical standards are developed primarily by the market participants, whereby fair participation must be ensured for all stakeholders. For this, an open forum should be established at an early stage where the participants (both those supplying and those requesting the data) are able to discuss the functional requirements for the interfaces as well as the technical issues. It should also be possible for rapid decisions to be made on controversial issues; the EBA's Q&A procedure is not entirely suitable for this: it is too slow, and the answers do not have a binding effect. Finally, significantly more attention needs to be paid to the aspect of testing. In addition to test environments, data requestors must also be given the option of accessing, via test accounts, the live systems at an early stage. Testing periods should also be significantly longer than stipulated in Delegated Regulation (EU) 2018/389.

- As with the comprehensive consideration of data protection requirements, the establishment of a data standard and a technical exchange standard is a fundamental prerequisite for open finance. In addition to this,

consumers must continue to retain control over their data and know what happens with this data.

- There must also be clarity regarding which undertakings have access to financial data, and which do not. And at what costs this is possible. These are basic principles for ensuring legal certainty on the exchange of data based upon which innovative business models can be established.

- Consideration is required regarding whether undertakings should be allowed to charge for the cost of providing data, and this could be differentiated in line with the value of the data, e.g. if this involves information generated by an undertaking (see also responses to Questions 31 and 32). With respect to payment transactions, the national legislator has also obliged other undertakings above a certain size to open up their technical infrastructure in return for a reasonable fee through section 58a of the Payment Services Supervision Act (ZAG). This legal provision could act as a model for appropriate regulation.

- If a mandatory, automated exchange of data is envisaged, then it should be implemented across all sectors wherever possible and also be interoperable, and not confined solely to the financial sector. This would enable cross-sectoral implementation of, as foreseen in the GDPR concept, the central right to data portability pursuant to Article 20 of the GDPR. This could further promote the strengthening of data protection, consumer protection and competition for data protection-friendly technologies and, above all, ultimately further strengthen people's control over their own data, as intended by European legislators through the right to data portability (see recital 68 of the GDPR).

And it could also strengthen the objective of Article 20 of the GDPR, stated by the Article 29 Data Protection Working Party, i.e. of making it easier for an affected person to smoothly move, copy or transfer their own personal data from one IT environment to another.

Having said that, consideration should also be given to the fact that any extension to the automated exchange of data and the inclusion of further players is also, at all times, accompanied by a correspondingly greater risk for data protection and/or data security.

Explanation to question 39

Financial Industry

A break-up of existing value chains and the emergence of new ones can be observed across all sectors, with previously internal processes of one single player now being spread across several market participants, also including previously unregulated ones. Concentration risks and a greater relevance of previously unregulated providers can increasingly arise for the financial market when central cloud service, software, data and platform providers provide identical or very similar bases for processes or algorithms to a large number of market participants. The concentration risks are enhanced through the emergence of lock-in effects with the third-party providers just described.

When using BDAI and designing (semi-)automated processes, it is important to guarantee that these are embedded in an effective, adequate and proper business organisation. The necessity of an appropriate level of competence in handling BDAI is self-evident here. According to the feedback from the consultation on BaFin's BDAI Study, the existing sector-specific regulation is stated as being generally adequate, although there is a need for clarification in some cases regarding how the existing rules should be applied with respect to BDAI.

When embedding these aspects in an effective, adequate and proper business organisation, the specific risks and requirements of complex BDAI models need to be considered (see Question 40 regarding the considerations on how the risks can be appropriately addressed and which measures are required):

Traceability, and with it also the internal and external verifiability of results, can be more difficult in the case of complex models.

Process automation based on BDAI can achieve a high level of scalability. This results in the risk that even minor errors can scale significantly and spread systematically.

The quality of the results of BDAI models is dependent, among other things, on the data used; correspondingly, data of an adequate quality and quantity must be available and be used.

Distorted results (bias) can occur systematically when deploying BDAI, thereby leading to incorrect decisions: there is a risk that, for instance, distorted/non-representative data are used; certain features in the modelling

phase may be either improperly under-weighted or over-weighted; distorted interpretations may also be provided despite correct algorithmic results.

The risk of unlawful discrimination can increase through the use of BDAI: algorithms might use features that must not be used on legal grounds for differentiation purposes. And even if no improper features are used, approximation of those improper features is still possible as very many other features are available that allow quite precise approximations.

In addition to the legal aspects, the increased reputational risks associated with the risks of “bias” and “risk of discrimination” must also be considered.

Managing information security risks faces new challenges as a result of the growing complexity caused by BDAI. The disaggregation of value chains supported by BDAI and the growing data volumes increase the attack surface for external access while at the same time reducing the individual provider’s ability to control the data used and distributed. In addition, certain BDAI algorithms can also suffer attacks through data manipulation. Examples include adversarial and poisoning attacks.

Consumers/Investor

The following risks arise in addition to the general risks in the financial industry as stated previously, which currently apply directly to consumers (bias, discrimination) and investors:

BDAI selection mechanisms (improved risk assessment, use of new data sources) could make it more difficult for certain consumers to access financial services. The question arises therefore as to how access to (affordable) financial services can be maintained if customers cannot or do not want to submit comprehensive (new) data sources (financial exclusion).

There is a risk that customers will not be informed in a sufficiently understandable and transparent manner about the potential reach and consequences of use of their data in conjunction with BDAI, and that they will de facto not have reliable controls and options available to them as a result.

The linking driven by BDAI of financial transaction and behavioural data with other data (sources) can facilitate the assessment of the willingness to pay. This would thus make it possible to exploit the customer’s (situational) willingness and ability to pay when setting prices if the provider is aware of

these. The formation of too few central customer interfaces caused by BDAI (see also statements on concentration risks) could additionally encourage these developments through improved data access and assessment synergies.

Supervisory authorities

In terms of supervision, the risks just described for the financial market, consumers and investors must be monitored with respect to technology-neutral regulation. Some of the risks stated previously do not only make in-house controls of BDAI models and their associated risks more difficult, but also the external verifiability, for instance by supervisory authorities.

The increasing complexity of the models used should be mentioned here: transparent selection processes and documentation of models are therefore important not only within an undertaking, but also represent a fundamental prerequisite for risk-based supervision. Fragmented value chains in particular make the supervision process even more difficult (see above for details): activities with similar risks should also be subject to similar supervision and regulation in the sense of an activity-based supervisory approach. A stronger focus on this approach could therefore be advisable in order to maintain a level playing field and to capture the existing risks adequately for regulatory purposes.

A corresponding understanding by the supervisory authorities and the existence of clear rules and interpretations of these rules are, of course, a fundamental prerequisite for risk-based supervision with increased use of BDAI.

Explanation to question 40

Based on the results of BaFin's BDAI study and the result of the consultation, it is possible to conclude that the existing sector-specific regulation and, in particular, the governance provisions are in general adequate for the use of BDAI models and therefore sufficient. The technology-neutral nature of the existing regulation is the main reason for this conclusion. Nevertheless, the feedback received gives rise to the need to explain certain aspects of the existing regulation and its interpretations in more detail with respect to the use of BDAI. The question arises, for instance, in this regard as to what represents a sufficient amount of transparency of a BDAI model, and how this can be guaranteed.

Certain clarifications of existing rules could help undertakings to guarantee clear procedures for fulfilling all requirements and, as a result, legal certainty when using BDAI. BaFin is for instance working to specify certain governance provisions in the context of BDAI in order to meet the needs for clarification.

This type of work by national supervisory authorities should subsequently be taken up by the ESAs so that these can publish guidelines for the interpretation of existing sector-specific regulation.

In terms of the considerations regarding new horizontal and/or cross-sectoral regulation, as listed in the Commission's White Paper on Artificial Intelligence, it should be noted that many of the White Paper's regulatory proposals are already contained in the existing supervisory governance and documentation requirements for financial market regulation. There is a risk of duplication or of contradictions with the existing financial market regulation, depending on the design of the additional horizontal regulation. This needs to be avoided, and the focus with the financial market should clearly be on sector-specific clarification. The cross-sectoral principles/requirements put forward in the White Paper could potentially represent a cross-sectoral minimum standard which complements the financial market regulation, in particular in the case of complex value chains. This would then be addressed primarily at those undertakings that make a contribution to these value chains without being subject to financial market regulation themselves (see Question 39 for details). However, the proposals in the White Paper on cross-sectoral standards would subsequently need to be substantiated.

According to the proposal in the White Paper, the horizontal requirements should be fulfilled in future by that player who is best able to deal with the potential risks of AI applications. This should for instance be developers for risks in the development phase of AI or operators when it comes to using the AI. With regard to this proposal, however, it should be noted that managerial responsibility always applies in the supervised undertakings of the financial sector, including, or, especially in distributed value chains. Improved interlinking of the proposals with existing financial regulation is therefore also necessary.

Contrary to the ex-ante conformity assessment (approval, certification) of risky AI applications or of algorithms in general put forward in the White Paper, in the existing financial regulation, approval (risk-oriented) is only

being given up until now for internal models for determining capital requirements. Other AI applications that are embedded in the decision-making processes and that have supervisory relevance are not covered on a technology-specific basis by ongoing supervision, but they are covered from a risk-oriented point of view as part of the general (technology-neutral) supervisory requirements for certain processes; however, these are not approved ex ante. A general approval of AI applications is, in BaFin's view, not necessary from a risk-oriented perspective nor does it make economic sense (see BaFin's position on a general approval of algorithm-based decision-making processes https://www.bafin.de/dok/13783136).

If a general ex-ante conformity assessment of a cross-sectoral nature is sought and to be completed by central enforcement panels (similar to the German Technical Inspection Association, TÜV), this could result in duplication and in worst case scenarios in contradictions with existing financial market regulation, unless a close interlinking with existing financial market regulation is ensured.

An ex-ante conformity assessment of cross-sectoral minimum standards should therefore only be implemented for the financial market as a supplementary requirement and not as a replacement of the existing financial market regulation. A further consideration when considering large scale ex-ante conformity assessments is that these would only be able to provide a very superficial review, simply as a result of the massive scale of algorithmic decision-making processes to be tested. As a result, these cannot be compared with the supervisory approval of internal models or reviews completed on an event-driven basis by financial supervision.