Chapter 9

Data reporting service

9.2B Operating requirements

Requirements for the management body of a data reporting service provider

9.2B.1 R The following requirements apply in respect of the *management body* of a *data reporting service provider*:

(1) The *management body* must possess adequate collective knowledge, skills and experience to be able to understand the activities of the *data reporting service provider*.

(2) The members of the *management body* must:

(a) be of sufficiently good repute;

(b) possess sufficient knowledge, skill and experience, and be able to commit sufficient time, to perform their duties; and

(c) act with honesty, integrity and independence of mind:

(i) to challenge effectively the decisions of the *senior management* where necessary; and

(ii) to oversee and effectively monitor management decision-making where necessary.

(3) The *management body* must:

(a) define and oversee the implementation of governance arrangements of the *data reporting service provider* to ensure the effective and prudent management of the provider, including the segregation of duties in the provider and the prevention of conflicts of interest; and

(b) when doing so, act in a manner that promotes the integrity of the financial markets and the interests of its clients.

(4) Where:

(a) an applicant for verification under regulation 7 of the *DRS Regulations* is a *recognised investment exchange*; and

(b) the *management body* of the applicant is the same as the *management body* of the exchange,

the requirements in (1) and (2) are deemed to be met.

Conflicts of interest

9.2B.2 R (1) A *data reporting services provider* must operate and maintain effective administrative arrangements, designed to prevent conflicts

of interest with clients using its services to meet their regulatory obligations, and other entities purchasing data from *data reporting services providers*. Such arrangements must include policies and procedures for identifying, managing and disclosing existing and potential conflicts of interest and must contain:

(a) an inventory of existing and potential conflicts of interest, setting out their description, identification, prevention, management and disclosure;

(b) the separation of duties and business functions within the *data reporting services provider*, including:

(i) measures to prevent or control the exchange of information where a risk of conflicts of interest may arise; and

(ii) the separate supervision of relevant *persons* whose main functions involve interests that are potentially in conflict with those of a client;

(c) a description of the fee policy for determining fees charged by the *data reporting services provider* and undertakings to which the *data reporting services provider* has *close links*;

(d) a description of the remuneration policy for the members of the *management body* and *senior management*; and

(e) the rules regarding the acceptance of money, gifts or favours by staff of the *data reporting services provider* and its *management body*.

(2) The inventory of conflicts of interest referred to in (1)(a) must include conflicts of interest arising from situations where the *data reporting services provider*:

(a) may realise a financial gain or avoid a financial loss, to the detriment of a client;

(b) may have an interest in the outcome of a service provided to a client, which is distinct from the client's interest in that outcome;

(c) may have an incentive to prioritise its own interests or the interests of another client or group of clients rather than the interests of a client to whom the service is provided; and

(d) receive or may receive from any *person* other than a client, in relation to the service provided to a client, an incentive in the form of money, goods or services, other than commission or fees received for the service.

Organisational requirements regarding outsourcing

9.2B.3 R (1) Where a *data reporting services provider* arranges for activities to be performed on its behalf by third parties, including undertakings with which it has *close links*, it must ensure that the third-party service provider has the ability and the capacity to perform the activities reliably and professionally.

(2) A *data reporting services provider* must specify which of the activities are to be outsourced, including a specification of the level of human and technical resources needed to carry out each of those activities.

(3) A *data reporting services provider* that outsources activities must ensure that the outsourcing does not reduce its ability or power to perform *senior management* or *management body* functions.

(4) A *data reporting services provider* must remain responsible for any outsourced activity and must adopt organisational measures to ensure:

(a) that it assesses whether the third-party service provider is carrying out outsourced activities effectively, and in compliance with applicable laws and regulatory requirements, and adequately addresses identified failures;

(b) the identification of the risks in relation to outsourced activities and adequate periodic monitoring;

(c) adequate control procedures with respect to outsourced activities, including effectively supervising the activities and their risks within the *data reporting services provider*; and

(d) adequate business continuity of outsourced activities.

(5) For the purposes of (4)(d), the *data reporting services provider* must obtain information on the business continuity arrangements of the third-party service provider, assess its quality and, where needed, request improvements.

(6) A *data reporting services provider* must ensure that the third-party service provider cooperates with the *FCA* in connection with outsourced activities.

(7) Where a *data reporting services provider* outsources any critical function, it must provide the *FCA* with:

(a) the identification of the third-party services provider;

(b) the organisational measures and policies with respect to outsourcing and the risks posed by it as specified in (4); and

(c) internal or external reports on the outsourced activities.

(8) For the purpose of ■ MAR 9.2B.3R(7), a function will be regarded as critical if a defect or failure in its performance would materially impair the continuing compliance of the *data reporting services provider* with the conditions and obligations of its authorisation or its other obligations under the *DRS Regulations* and this chapter.

Business continuity and back-up facilities

9.2B.4 R

(1) A *data reporting services provider* must use systems and facilities that are appropriate and robust enough to ensure continuity and regularity in the performance of the services provided as referred to in this chapter.

(2) A *data reporting services provider* must conduct periodic reviews, at least annually, evaluating its technical infrastructures and associated policies and procedures, including business continuity arrangements. A *data reporting services provider* must remedy any deficiencies identified during the review.

(3) A *data reporting services provider* must have effective business continuity arrangements in place to address disruptive incidents, including:

(a) the processes which are critical to ensuring the services of the *data reporting services provider*, including escalation procedures, relevant outsourced activities and dependencies on external providers;

(b) specific continuity arrangements, covering an adequate range of possible scenarios, in the short and medium term, including system failures, natural disasters, communication disruptions, loss of key staff and an inability to use the premises regularly used;

(c) duplication of hardware components, allowing for failover to a back-up infrastructure, including network connectivity and communication channels;

(d) back-up of business-critical data and up-to-date information of the necessary contacts, ensuring communication within the *data reporting services provider* and with clients;

(3) the procedures for moving to and operating *data reporting services* from a back-up site;

(f) the target maximum recovery time for critical functions, which must be as short as possible and, in any case, no longer than 6 hours in the case of *approved publication arrangements* (*APAs*) and *consolidated tape providers* (*CTPs*) and until the close of business of the next working day in the case of *approved reporting mechanisms* (*ARMs*); and

(g) staff training on the operation of the business continuity arrangements, individuals' roles, including specific security operations personnel ready to react immediately to a disruption of services.

(4) A *data reporting services provider* must set up a programme for periodically testing, reviewing and, where needed, modifying the business continuity arrangements.

(5) A *data reporting services provider* must publish on its website and promptly inform its clients and the *FCA* of any service interruptions or connection disruptions as well as the time estimated to resume a regular service.

Testing and capacity

9.2B.5 R (1) A *data reporting services provider* must implement clearly delineated development and testing methodologies, ensuring that:

(a) the operation of the IT systems satisfies the *data reporting services provider's* regulatory obligations;

(b) compliance and risk management controls embedded in IT systems work as intended; and

(c) the IT systems can continue to work effectively at all times.

(2) A *data reporting services provider* must also use the methodologies referred to in (1) prior to and following the deployment of any updates of the IT systems.

(3) A *data reporting services provider* must promptly notify the *FCA* of any planned significant changes to the IT systems prior to their implementation.

(4) A *data reporting services provider* must set up an ongoing programme for periodically reviewing and, where needed, modifying the development and testing methodologies.

(5) A *data reporting services provider* must run stress tests periodically and at least on an annual basis. A *data reporting services provider* must include in the adverse scenarios of the stress test unexpected behaviour of critical constituent elements of its systems and communications lines. The stress testing must identify how hardware, software and communications respond to potential threats, specifying systems unable to cope with adverse scenarios. A *data reporting services provider* must take measures to address identified shortcomings in those systems.

(6) A *data reporting services provider* must:

(a) have sufficient capacity to perform its functions without outages or failures, including missing or incorrect data; and

(b) have sufficient scalability to accommodate without undue delay any increase in the amount of information to be processed and in the number of access requests from its clients.

Security

9.2B.6 R

(1) A *data reporting services provider* must set up and maintain procedures and arrangements for physical and electronic security designed to:

(a) protect its IT systems from misuse or unauthorised access;

(b) minimise the risks of attacks against *information systems*;

(c) prevent unauthorised disclosure of confidential information; and

(d) ensure the security and integrity of the data.

(2) Where a *MiFIR investment firm* ('reporting firm') uses a third party to submit information to an *ARM* on its behalf ('submitting firm'), the *ARM* must have procedures and arrangements in place to ensure that the submitting firm does not have access to any other information about, or submitted by, the reporting firm to the *ARM* which may have been sent by the reporting firm directly to the *ARM* or through another submitting firm.

(3) A *data reporting services provider* must set up and maintain measures and arrangements to promptly identify and manage the risks identified in (1).

(4) In respect of breaches in the physical and electronic security measures referred to in (1) to (3), a *data reporting services provider* must promptly notify:

(a) the *FCA* and provide an incident report, indicating the nature of the incident, the measures adopted to cope with the incident and the initiatives taken to prevent similar incidents; and

(b) its clients that have been affected by the security breach.

Record keeping

9.2B.7 R

(1) A *data reporting service provider* must maintain records, in retrievable and legible form, of information that could be relevant to demonstrating its compliance or non-compliance with any requirement imposed by the *rules* in this chapter.

(2) A *data reporting service provider* must retain the records for no less than 5 years from the date on which the records were created.

Reporting of infringements

9.2B.8 R

A *data reporting service provider* must have in place effective procedures for its employees to report potential or actual infringements of:

(1) the *rules*;

(2) *MiFIR*, and any *onshored regulations* previously deriving from *MiFIR* or *MiFID*; and

(3) the *DRS Regulations*,

internally through a specific, independent and autonomous channel.

Conditions for an ARM

9.2B.9 R

(1) An *ARM* must have adequate policies and arrangements in place to enable it to report the information required from a *MiFIR investment firm* under article 26 of *MiFIR* as quickly as possible and no later than 11:59pm on the *working day* following the *day* on which the transaction took place.

(2) The information mentioned in (1) must be reported in accordance with article 26 of *MiFIR*.

(3) An *ARM* must:

(a) operate and maintain effective administrative arrangements designed to prevent conflicts of interest with its clients;

(b) have sound security mechanisms in place designed to:

(i) guarantee the security and authentication of the means of the transfer of information;

(ii) minimise the risk of data corruption and unauthorised access;

(iii) prevent information leakage; and

(iv) maintain the confidentiality of the data at all times;

(c) maintain adequate resources and have back-up facilities in order to offer and maintain its services at all times; and

(d) have systems which:

(i) effectively check *transaction reports* for completeness;

(ii) identify omissions and obvious errors caused by the *MiFIR investment firm*;

(iii) communicate details of such omissions or errors to the *MiFIR investment firm* and request re-transmission of erroneous reports;

(iv) detect omissions or errors caused by the *ARM* itself; and

(v) enable the *ARM* to correct and transmit, or retransmit, correct and complete *transaction reports* to the *FCA*.

(4) An *ARM* which is also a *recognised investment exchange* or a *MiFID investment firm* must treat all information collected in a non-discriminatory fashion and must operate and maintain appropriate arrangements to separate different business functions.

Management of incomplete or potentially erroneous information by ARMs

9.2B.10 R

(1) An *ARM* must set up and maintain appropriate arrangements to identify *transaction reports* that are incomplete or contain obvious errors caused by clients. An *ARM* must perform validation of the *transaction reports* against the requirements established under article 26 of *MiFIR* for field, format and content of fields in accordance with Table 1 of Annex I to *MiFID RTS 22*.

(2) An *ARM* must set up and maintain appropriate arrangements to identify *transaction reports* which contain errors or omissions caused by that *ARM* itself and to correct, including deleting or amending, such errors or omissions. An *ARM* must perform validation for field, format and content of fields in accordance with Table 1 of Annex I to *MiFID RTS 22*.

(3) An *ARM* must continuously monitor in real time the performance of its systems, ensuring that a *transaction report* it has received has been successfully reported to the *FCA* in accordance with article 26 of *MiFIR*.

(4) An *ARM* must perform periodic reconciliations at the request of the *FCA* between the information that the *ARM* receives from its client or generates on the client's behalf for *transaction reports* purposes and data samples of the information provided by the *FCA*.

(5) Any corrections, including cancellations or amendments of *transaction reports* that are not correcting errors or omissions caused by an *ARM*, must only be made at the request of a client and per *transaction report*. Where an *ARM* cancels or amends a *transaction report* at the request of a client, it must provide this updated *transaction report* to the client.

(6) Where an *ARM*, before submitting the *transaction report*, identifies an error or omission caused by a client, it must not submit that *transaction report* and must promptly notify the *MiFIR investment firm* of the details of the error or omission to enable the client to submit a corrected set of information.

(7) Where an *ARM* becomes aware of errors or omissions caused by the *ARM* itself, it must promptly submit a correct and complete report.

(8) An *ARM* must promptly notify the client of the details of the error or omission and provide an updated *transaction report* to the client. An *ARM* must also promptly notify the *FCA* about the error or omission.

(9) The requirement to correct or cancel erroneous *transaction reports* or report omitted transactions must not extend to errors or omissions which occurred more than 5 years before the date that the *ARM* became aware of such errors or omissions.

Connectivity of ARMs

9.2B.11 R (1) An *ARM* must have in place policies, arrangements and technical capabilities to comply with the technical specification for the submission of transaction reports required by the *FCA*.

(2) An *ARM* must have in place adequate policies, arrangements and technical capabilities to receive *transaction reports* from clients and to transmit information back to clients. The *ARM* must provide the client with a copy of the *transaction report* which the *ARM* submitted to the *FCA* on the client's behalf.

Conditions for an APA – organisational requirements

9.2B.12 R (1) An *APA* must:

(a) have sound security mechanisms in place designed to:

(i) guarantee the security of the means of the transfer of information;

(ii) minimise the risk of data corruption and unauthorised access; and

(iii) prevent information leakage before publications;

(b) maintain adequate resources and have back-up facilities in order to offer and maintain its services at all times; and

(c) have systems which can effectively:

(i) check trade reports for completeness;

(ii) identify omissions and obvious errors; and

(iii) request re-transmission of any erroneous reports.

(2) An *APA* which is also a *recognised investment exchange* or a *MiFID investment firm* must treat all information collected in a non-discriminatory fashion and must operate and maintain appropriate arrangements to separate different business functions.

Conditions for a CTP – organisational requirements

9.2B.13 R A *CTP* must:

(1) have sound security mechanisms in place designed to:

(a) guarantee the security of the means of the transfer of information; and

(b) minimise the risk of data corruption and unauthorised access; and

(2) maintain adequate resources and have back-up facilities in order to offer and maintain its services at all times.

Other services provided by CTPs

9.2B.14 R (1) A *CTP* for bonds must not provide any additional service which utilises the information it receives from *UK trading venues* and *APAs* in its capacity as a *CTP*.

(2) Where a *CTP* for bonds is a member of a *group*, a member of that *group* may provide an additional service utilising information from the consolidated tape for bonds, provided it has paid for that information in accordance with ■ MAR 9.2B.36R(1).

Management of incomplete or potentially erroneous information by APAs

9.2B.15 R (1) *APAs* must set up and maintain appropriate arrangements to ensure that they accurately publish the trade reports received from *MiFIR investment firms* without themselves introducing any errors or omitting information and must correct information where they have themselves caused the error or omission.

(2) *APAs* must continuously monitor in real-time the performance of their IT systems ensuring that the trade reports they have received have been successfully published.

(3) *APAs* must perform periodic reconciliations between the trade reports that they receive and the trade reports that they publish, verifying the correct publication of the information.

(4) An *APA* must confirm the receipt of a trade report to the reporting *MiFIR investment firm*, including the transaction identification code assigned by the *APA*. An *APA* must refer to the transaction identification code in any subsequent communication with the reporting firm in relation to a specific trade report.

(5) An *APA* must set up and maintain appropriate arrangements to identify on receipt trade reports that are incomplete or contain information that is likely to be erroneous. These arrangements must include automated price and volume alerts, taking into account:

(a) the sector and the segment in which the *financial instrument* is traded;

(b) liquidity levels, including historical trading levels;

(c) appropriate price and volume benchmarks; and

(d) if needed, other parameters according to the characteristics of the *financial instrument*.

(6) Where an *APA* determines that a trade report it receives is incomplete or contains information that is likely to be erroneous, it must not

publish that trade report and must promptly alert the *MiFIR investment firm* submitting the trade report.

(7) In exceptional circumstances, *APAs* must delete and amend information in a trade report on request from the entity providing the information when that entity cannot delete or amend its own information for technical reasons. *APAs* are not otherwise responsible for correcting information contained in published reports where the error or omission was attributable to the entity providing the information.

(8) *APAs* must publish non-discretionary policies on information cancellation and amendments in trade reports which set out the penalties that *APAs* may impose on *MiFIR investment firms* providing trade reports where the incomplete or erroneous information has led to the cancellation or amendment of trade reports.

Conditions for an APA – policies and arrangements for publication of information

9.2B.16 R

(1) An *APA* must have adequate policies and arrangements in place to make public the information required under articles 20 and 21 of *MiFIR* in as close to real time as is technically possible on a reasonable commercial basis.

(2) The information referred to in (1) must be made available by the *APA* free of charge 15 minutes after the *APA* has first published it.

(3) The *APA* must be able to disseminate efficiently and consistently the information referred to in (1):

(a) in a way which ensures fast access to the information on a non-discriminatory basis; and

(b) in a format that facilitates the consolidation of the information with similar data from other sources.

(4) The information referred to in (1) must include the following details:

(a) the identifier of the *financial instrument*;

(b) the price at which the transaction was concluded;

(c) the volume of the transaction;

(d) the time of the transaction;

(e) the time the transaction was reported;

(f) the price notation of the transaction;

(g) the code for the trading venue the transaction was executed on or, where the transaction was executed on a *systematic internaliser*, the code 'SI' or, otherwise, '*OTC*'; and

(h) if applicable, an indicator that the transaction was subject to specific conditions.

Machine readability – APAs

9.2B.17 R

(1) *APAs* must publish the information which has to be made public in accordance with ■ MAR 9.2B.16R(1) in a machine-readable way.

(2) Information is published in a machine-readable way where all of the following conditions are met:

(a) it is in an electronic format designed to be directly and automatically read by a computer;

(b) it is stored in an appropriate IT architecture, in accordance with MAR 9.2B.5R(6), that enables automatic access;

(c) it is robust enough to ensure continuity and regularity in the performance of the services provided and ensures adequate access in terms of speed; and

(d) it can be accessed, read, used and copied by computer software that is free of charge and publicly available.

(3) For the purposes of (2)(a), the electronic format must:

(a) be specified by free, non-proprietary and open standards; and

(b) include the type of files of messages, the rules to identify them, and the name and data type of the fields they contain.

(4) APAs must:

(a) make instructions available to the public, explaining how and where to easily access and use the data, including identification of the electronic format;

(b) make public any changes to the instructions referred to in (4)(a) at least 3 *months* before they come into effect, unless there is an urgent and duly justified need for changes in instructions to take effect more quickly; and

(c) include a link to the instructions referred to in (4)(a) on the homepage of their website.

9

Certification requirement

9.2B.18 R An *APA* must require each *MiFIR investment firm* to certify that it only reports transactions in a particular *financial instrument* through that *APA*.

Details to be published by the APA

9.2B.19 R (1) An *APA* must make public:

(a) for transactions executed in respect of shares, depositary receipts, *exchange-traded funds* (*ETFs*), *certificates* and other similar *financial instruments*, the details of a transaction specified in Table 2 of Annex I to *MiFID RTS 1* and use the appropriate flags listed in Table 3 of Annex I to *MiFID RTS 1*; and

(b) for transactions executed in respect of bonds, *structured finance products*, *emission allowances* and derivatives, the details of a transaction specified in Table 1 of Annex II to *MiFID RTS 2* and use the appropriate flags listed in Table 2 of Annex II to *MiFID RTS 2*.

(2) Where publishing information on when the transaction was reported, an *APA* must include the date and time, up to the second, it publishes the transaction.

(3) By way of derogation from ■ MAR 9.2B.19R(2), an *APA* that publishes information regarding a transaction executed on an electronic system must include the date and time, up to the millisecond, of the publication of that transaction in its trade report.

(4) For the purposes of (3), an 'electronic system' means a system where orders are electronically tradable or where orders are tradable outside the system, provided that they are advertised through the given system.

(5) The timestamps referred to in (2) and (3) must, respectively, not diverge by more than one second or millisecond from the Coordinated Universal Time (UTC) issued and maintained by one of the timing centres listed in the latest Bureau International des Poids et Mesures (BIPM) Annual Report on Time Activities.

Non-discrimination requirements for APAs

9.2B.20 R *APAs* must ensure that the information which must be made public is sent through all distribution channels at the same time, including when the information is made public, as close to real time as technically possible or 15 minutes after the first publication.

Obligation on APAs to provide market data on a reasonable commercial basis

9.2B.21 R (1) For the purposes of making market data containing the information set out in articles 6, 20 and 21 of *MiFIR* available to the public on a reasonable commercial basis and in accordance with ■ MAR 9.2B.16R(1), *APAs* must comply with the obligations set out in ■ MAR 9.2B.22R to ■ MAR 9.2B.26R.

(2) The obligations set out in ■ MAR 9.2B.22R, ■ MAR 9.2B.23R(2), ■ MAR 9.2B.24R, ■ MAR 9.2B.25R(2) and ■ MAR 9.2B.26R do not apply to *APAs* that make market data available to the public free of charge.

Provision of market data based on cost – APAs

9.2B.22 R (1) The price of market data must be based on the cost of producing and disseminating such data and may include a reasonable margin.

(2) The costs of producing and disseminating market data may include an appropriate share of joint costs for other services provided by *APAs*.

Obligation to provide market data on a non-discriminatory basis – APAs

9.2B.23 R (1) *APAs* must make market data available at the same price and on the same terms and conditions to all customers falling within the same category in accordance with published objective criteria.

(2) Any differentials in prices charged to different categories of customers must be proportionate to the value which the market data represent to those customers, taking into account:

(a) the scope and scale of the market data, including the number of *financial instruments* covered and trading volume; and

(b) the use made by the customer of the market data, including whether it is used for the customer's own trading activities, for resale or for data aggregation.

(3) For the purposes of MAR 9.2B.23R(1), *APAs* must have scalable capacities in place to ensure that customers can obtain timely access to market data at all times on a non-discriminatory basis.

Per user fees – APAs

9.2B.24 R

(1) *APAs* must charge for the use of market data on the basis of the use made by individual end-users of the market data ('per user basis'). *APAs* must have arrangements in place to ensure that each individual use of market data is charged only once.

(2) By way of derogation from MAR 9.2B.24R(1), *APAs* may decide not to make market data available on a per user basis where to charge on a per user basis is disproportionate to the cost of making market data available, having regard to the scale and scope of the market data.

(3) *APAs* must provide grounds for the refusal to make market data available on a per user basis and must publish those grounds on their webpage.

9

Unbundling and disaggregating market data – APAs

9.2B.25 R

(1) *APAs* must make market data available without being bundled with other services.

(2) Prices for market data must be charged on the basis of the level of market data disaggregation provided for in article 12(1) of *MiFIR* as further specified in articles of *MiFID RTS 14*.

Transparency obligation – APAs

R

(1) *APAs* must disclose and make easily available to the public the price and other terms and conditions for the provision of the market data in a manner which is easily accessible.

(2) The disclosure must include the following:

(a) current price lists and other contractual terms and conditions; and

(b) advance disclosure with a minimum of 90 *days*' notice of future price changes.

Conflicts of interest obligations for CTPs

9.2B.27 R

(1) Where a *CTP* is a member of a *group*, the arrangements it establishes to prevent or manage conflicts of interest in accordance with MAR 9.2B.2R(1) must also take into account any circumstances, of which the *CTP* is or should be aware, which may give rise to a conflict of interest arising as a result of the structure and business activities of other members of the *group*.

(2) A *CTP* must assess and periodically review, on an at least annual basis, the conflicts of interest policies and procedures established in accordance with ■ MAR 9.2B.2R(1) and must take all appropriate measures to address any deficiencies.

(3) A *CTP* must keep and regularly update a record of the kinds of services or activity it carries on in which a conflict of interest entailing a risk of damage to the interests of one or more clients has arisen, or in the case of an ongoing service or activity, may arise. *Senior management* of the *CTP* must receive on a frequent basis, and at least annually, written reports on these records and how any conflicts have been managed.

Obligations for CTPs on apportionment of responsibilities

R A *CTP* must take reasonable care to maintain a clear and appropriate apportionment of significant responsibilities among its *senior management* in such a way that:

(1) it is clear who has which of those responsibilities; and

(2) the business and affairs of the *CTP* can be adequately monitored and controlled by its directors, senior managers and *management body* of the *CTP*.

Outsourcing obligations for CTPs

9.2B.29 R (1) In addition to complying with its obligations under ■ MAR 9.2B.3R(6), a *CTP* must provide the *FCA* with a written agreement in respect of any arrangement it enters into with a third-party provider to outsource a critical function. The agreement must contain a clear allocation of the respective rights and obligations of the *CTP* and the third-party provider.

(2) In relation to the arrangement referred to in (1), the *CTP* must take the necessary steps to ensure it is able to:

(a) terminate that arrangement where necessary, with immediate effect, without detriment to the continuity and quality of its provision of services; and

(b) cooperate with the *FCA*, including providing information to the *FCA* on request, and putting in place arrangements enabling the *FCA* to seek information from the third-party provider.

Non-discrimination obligations for CTPs

9.2B.30 R Any of the following *persons* who are also a *CTP* must treat all information collected in a non-discriminatory fashion and must operate and maintain appropriate arrangements to separate different business functions:

(1) a *recognised investment exchange*;

(2) an *APA*;

(3) an *investment firm*;

(4) a *data vendor*; or

(5) a *firm* whose *shares* or voting rights are at least 20% owned by a *person* referred to in (1) to (4) or who shares a business function with such a *person*.

Management of incomplete or potentially erroneous information by CTPs

9.2B.31 R (1) A *CTP* must set up and maintain appropriate arrangements to ensure that it accurately publishes the trade reports received from *MiFIR investment firms*, *regulated markets* and *APAs* without itself either:

(a) introducing any errors that would affect the accuracy and completeness of the data contained in those reports; or

(b) omitting any information from those reports, except where such omission is a deliberate one in accordance with the *CTP's* regulatory and contractual obligations.

(2) A *CTP* must correct information where it has itself introduced an error or made a non-deliberate omission as referred to in (1).

(3) A *CTP* must perform periodic reconciliations between the trade reports it receives and the trade reports it publishes, verifying the correct publication of the information.

9

Obligations of CTPs to ensure data quality and report information

9.2B.32 R (1) A *CTP* must continuously monitor in real time the performance of its IT systems and ensure that the trade reports it has received have been successfully published.

(2) A *CTP* must set up and maintain appropriate arrangements to identify on receipt trade reports that are incomplete or contain information that is likely to be erroneous, and must inform the provider of the trade report in each instance.

(3) In exceptional circumstances, a *CTP* must delete and amend information in a trade report on request from the entity providing the information when that entity cannot delete or amend its own information for technical reasons. *CTPs* are not otherwise responsible for correcting information contained in published reports where the error or omission was attributable to the entity providing the information.

(4) The *CTP* must submit a report to the *FCA* every 6 *months* on the quality of the data that it has received during that period. The report must include at least the following information:

(a) the timeliness of the receipt of data from data contributors;

(b) the timeliness of publication of information by the *CTP*;

(c) details of the trade reports that are incomplete or contain information that is likely to be erroneous that have been identified;

(d) whether the *CTP* has correctly published the information it has received;

(e) the performance of the *CTP's* IT systems; and

(f) the usage of the consolidated tape.

Consolidation of data by CTPs

9.2B.33 R A *CTP* must:

(1) ensure that the data it makes available publicly is consolidated from all *UK trading venues* and *APAs* into a continuous electronic data stream;

(2) ensure that the information which must be made public is sent through all distribution channels at the same time, including when the information is made public, as close to real time as technically possible or 15 minutes after the first publication; and

(3) provide the *FCA* with direct and immediate access to the *consolidated tape for bonds*.

Scope of the consolidated tape for bonds and publication of information

9.2B.34 R (1) The *CTP* for bonds must have adequate policies and arrangements in place to:

(a) receive the information made public in accordance with articles 10 and 21 of *MiFIR* by all *UK trading venues* and *APAs* in respect of bonds excluding exchange traded commodities and exchange traded notes; and

(b) make that information available to the public in as close to real time as is technically possible or 15 minutes after the first publication.

(2) The *CTP* for bonds must have adequate policies and arrangements in place to make *historical data* available in response to a request for it in accordance with ■ MAR 9.2B.35R(2).

(3) The information referred to in (1) must include the details of a transaction specified in Table 1 of Annex II to *MiFID RTS 2* and use the appropriate flags listed in Table 2 of Annex II to *MiFID RTS 2*.

(4) Following the appointment of a provider of a *consolidated tape for bonds*, *UK trading venues* and *APAs* must:

(a) connect to the *CTP* for bonds before commencing or continuing operations; and

(b) send to the *CTP* for bonds, in as close to real time as is technically possible using the means established in ■ MAR 9.2B.34R(5) by the *CTP*, the information referred to in (1)(a).

(5) The *CTP* for bonds must operate an open-source Application Programming Interface (API) in order to receive the information referred to in (1)(a) from *UK trading venues* and *APAs*.

9

(6) The *CTP* for bonds must be able to disseminate the information referred to in (1)(a) efficiently, consistently and in way that:

(a) ensures fast access to the information on a non-discriminatory basis; and

(b) is in a generally accepted format that is interoperable, easily accessible and utilisable for market participants.

(7) When a new *UK trading venue* or *APA* starts operating, the *CTP* for bonds must include the information referred to in (1)(a) made public by that *UK trading venue* or *APA* in the electronic data stream of its consolidated tape as soon as possible after the start of the operations of the *UK trading venue* or *APA*.

(8) The *CTP* for bonds must not consolidate trade reports with the code "DUPL" in the reprint field.

Machine readability and required formats for CTPs for bonds

9.2B.35 R (1) The *CTP* for bonds must publish the information referred to in MAR 9.2B.34R(1) in Graphical User Interface (GUI) and at least 2 machine-readable formats: Application Programming Interface (API) and Comma Separated Value (CSV).

(2) The *CTP* for bonds must make *historical data* available in response to a request for it in GUI and one machine-readable format.

(3) Information is published in a machine-readable format where all of the following conditions are met:

(a) it is in an electronic format designed to be directly and automatically read by a computer;

(b) it is stored in an appropriate IT architecture, in accordance with MAR 9.2B.5R(6), that enables automatic access;

(c) it is robust enough to ensure continuity and regularity in the performance of the services provided and ensures adequate access in terms of speed; and

(d) it can be accessed, read, used and copied by computer software that is free of charge and publicly available.

(4) For the purposes of MAR 9.2B.35R(3)(a), the electronic format must be specified by free, non-proprietary and open standards, and include the type of files or messages, the rules to identify them, and the name and data type of the fields they contain.

(5) The *CTP* for bonds must:

(a) make instructions available to the public, explaining how and where to easily access and use the data, including identification of the electronic format;

(b) make public any changes to the instructions referred to in (5)(a) at least 3 *months* before they come into effect, unless there is an urgent and duly justified need for changes in instructions to take effect more quickly; and

(c) include a link to the instructions referred to in (5)(a) on the homepage of their website.

Obligation for the CTP for bonds to provide market data on a non-discriminatory basis

9.2B.36 R

(1) The *CTP* for bonds must make market data available at the same price and on the same terms and conditions to all customers falling within the same category in accordance with published objective criteria.

(2) The *CTP* for bonds must charge for the use of *historical data* when it is requested separately from the use of market data, except where it is provided in a machine-readable form through an API.

(3) For the purposes of ■ MAR 9.2B.36R(1), the *CTP* for bonds must have scalable capacities in place to ensure that customers can obtain timely access to market data at all times on a non-discriminatory basis.

9.2B.37 R [deleted]

Unbundling market data for the CTP for bonds

9.2B.38 R The *CTP* for bonds must make market data available without being bundled with other services.

Transparency obligations for the CTP for bonds

9.2B.39 R

(1) The *CTP* for bonds must disclose and make easily available to the public the price and other terms and conditions for the provision of the market data in a manner which is easily accessible.

(2) The disclosure must include the following:

(a) current price lists and other contractual terms and conditions; and

(b) advance disclosure with a minimum of 90 *days*' notice of future price changes.

Governance obligations for the CTP

9.2B.40 R

(1) The *CTP* must establish a consultative committee composed of a representative range of its users and data producers. *CTP* users and data producers may apply to the *CTP* to be members of the committee.

(2) The membership of the committee established in (1) must be renewed at least once during the period of tender for the *CTP*. At all times, users must comprise the majority of members on the committee.

(3) The committee must meet at least every 6 *months*, and its chair must make the meeting agenda and minutes public.

(4) The *CTP* must share with the committee, at a minimum, information on the following:

(a) its operating costs, including providing regular updates about those costs;

(b) its operational performance;

(c) its fee and user policies, including any changes to those policies usage of its services;

(d) usage of its services;

(e) any data quality issues; and

(f) any technology updates.

(5) The committee may make recommendations to the *CTP*. The chair must make public information on how the *CTP* is taking forward the recommendations of the committee, including on its performance and operation. If the *CTP* decides not to take forward a recommendation, it must provide the committee with reasons for its decision.