Changes to legislation: *There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2017/571. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2017 No. 571 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

Commission Delegated Regulation (EU) 2017/571 of 2 June 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards on the authorisation, organisational requirements and the publication of transactions for data reporting services providers (Text with EEA relevance)

COMMISSION DELEGATED REGULATION (EU) 2017/571

of 2 June 2016

supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards on the authorisation, organisational requirements and the publication of transactions for data reporting services providers

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 2014/65/EU of 15 May 2014 of the European Parliament and of the Council on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU[(1)], and in particular Article 61(4), Article 64(6) and (8), Article 65(6) and (8), and Article 66(5) thereof,

Whereas:

(1) In accordance with Directive 2014/65/EU data reporting services providers cover three different types of entities: approved reporting mechanisms (ARMs), approved publication arrangements (APAs) and consolidated tape providers (CTPs). Although those types of entities are engaged in different activities, Directive 2014/65/EU provides for a similar authorisation process for all of those entities.

(2) An applicant seeking authorisation as a data reporting services provider should provide in its application for authorisation a programme of operations and an organisational chart. The organisational chart should identify who is responsible for the different activities to enable the competent authority to assess whether the data reporting services provider has sufficient human resources and oversight over its business. The organisational chart should not only cover the scope of the data reporting services, but should also include any other services that the entity provides as this may highlight areas which may affect the independence of the data reporting services provider and give rise to a conflict of interest. An applicant seeking authorisation as a data reporting services provider should also provide information on the composition, functioning and independence of its governing bodies in order for competent authorities to be able to assess whether the policies, procedures and corporate governance structure ensure the independence of the data reporting services provider and the avoidance of conflicts of interest.

Changes to legislation: *There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2017/571. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2017 No. 571 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

(3) Conflicts of interest can arise between the data reporting services provider and clients using its services to meet their regulatory obligations and other entities purchasing data from data reporting services providers. In particular, those conflicts may arise where the data reporting services provider is engaged in other activities such as acting as a market operator, investment firm or trade repository. If conflicts are left unaddressed, this could lead to a situation where the data reporting services provider has an incentive to delay publication or submission of data or to trade on the basis of the confidential information it has received. The data reporting services provider should therefore adopt a comprehensive approach to identifying, preventing and managing existing and potential conflicts of interest, including preparing an inventory of conflicts of interest and implementing appropriate policies and procedures to manage those conflicts and, where necessary, separate business functions and personnel to limit the flow of sensitive information between different business areas of the data reporting services provider.

(4) All members of the management body of a data reporting services provider should be persons who are of sufficiently good repute and possess sufficient knowledge, skills and experience, as those persons play a key role in ensuring that the data reporting services provider meets its regulatory obligations and contribute to the business strategy of the data reporting services provider. It is therefore important for the data reporting services provider to demonstrate that it has a robust process for appointing and evaluating the performance of members of the management body and that clear reporting lines and regular reporting to the management body are in place.

(5) The outsourcing of activities, in particular of critical functions, is capable of constituting a material change of the conditions for the authorisation of a data reporting services provider. To ensure that the outsourcing of activities does not impair the data reporting services provider's ability to meet its obligations under Directive 2014/65/EU or lead to conflicts of interest, the data reporting services provider should be able to demonstrate sufficient oversight and control over those activities.

(6) The IT systems used by a data reporting services provider should be well adapted to the different types of activities those entities may perform, that is to publish trade reports, submit transaction reports or provide a consolidated tape, and robust enough to ensure continuity and regularity in the provision of those services. This includes ensuring that the data reporting services provider's IT systems are able to handle fluctuations in the amount of data which it must handle. Such fluctuations, particularly unexpected increases in data flow, may adversely impact the effectiveness of the data reporting services provider's systems and as a result, its ability to publish or report complete and accurate information within the required timeframes. In order to handle this, a data reporting services provider should periodically test its systems to ensure that they are robust enough to handle changes in operating conditions and sufficiently scalable.

(7) The backup facilities and arrangements established by a data reporting services provider should be sufficient to enable the data reporting services provider to deliver its services, even in the event of a disruptive incident. A data reporting services provider should establish maximum acceptable recovery times for critical functions that would apply in

***Changes to legislation:** There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2017/571. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2017 No. 571 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

the event of a disruptive incident, which should allow compliance with the deadlines for reporting and disclosing the information.

(8) To ensure that the data reporting services provider can provide its services, it should undertake an analysis of which tasks and activities are critical to the delivery of its services and of possible scenarios that may give rise to a disruptive incident, including taking steps to prevent and mitigate those situations.

(9) Where a service disruption occurs, a data reporting services provider should notify the competent authority of its home Member State, any other relevant competent authorities, clients and the public as the disruption could also mean that those parties would not be able to fulfil their own regulatory obligations such as the duty to forward transaction reports to other competent authorities or to make public the details of executed transactions. The notification should allow those parties to make alternative arrangements for meeting their obligations.

(10) The deployment of any IT systems' updates may potentially impact the effectiveness and robustness of the systems used for data service provision. To prevent that the operation of its IT system is at any time incompatible with its regulatory obligations, in particular that of having a sound security mechanism in place designed to guarantee the security of the means of transfer of information, minimise the risk of data corruption and to prevent information leakage before publication, a data reporting services provider should make use of clearly delineated development and testing methodologies to ensure that compliance and risk management controls embedded in the systems work as intended and that the system can continue to work effectively in all conditions. Where a data reporting services provider undertakes a significant system change, it should notify the competent authority of its home Member State and other competent authorities, where relevant, so they can assess whether the update will impact their own systems and whether the conditions for authorisation continue to be met.

(11) Premature public disclosure, in the case of trade reports, or unauthorised disclosure in the case of transaction reports could provide an indication of trading strategy or reveal sensitive information such as the identity of the data reporting services provider's clients. Therefore, physical controls, such as locked facilities, and electronic controls including firewalls and passwords should be put in place by the data reporting services provider to ensure that only authorised personnel have access to the data.

(12) Breaches in the physical or electronic security of a data reporting services provider pose a threat to the confidentiality of client data. Consequently, where such a breach occurs, a data reporting services provider should promptly notify the relevant competent authority as well as any clients which have been affected by the breach. Notification to the competent authority of the home Member State is necessary to enable that competent authority to carry out its ongoing supervisory responsibilities with respect to whether the data reporting services provider is properly maintaining sound security mechanisms to guarantee the security of the information and to minimise the risk of data corruption and unauthorised access. Other competent authorities which have a technical interface with the data reporting services provider should also be notified as they may be adversely

Changes to legislation: *There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2017/571. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2017 No. 571 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

affected, particularly where the breach relates to the means of transferring information between the data reporting services provider and the competent authority.

(13) An investment firm which has transaction reporting obligations, known as a 'reporting firm', may choose to use a third party to submit transaction reports on its behalf to an ARM, that is a 'submitting firm'. By virtue of its role the submitting firm will have access to the confidential information that it is submitting. However, the submitting firm should not be entitled to access any other data about the reporting firm or the reporting firm's transactions which are held at the ARM. Such data may relate to transaction reports which the reporting firm has submitted itself to the ARM or which it has sent to another submitting firm to send to the ARM. This data should not be accessible to the submitting firm as it may contain confidential information such as the identity of the reporting firm's clients.

(14) A data reporting services provider should monitor that the data it is publishing or submitting is accurate and complete and should ensure that it has mechanisms for detecting errors or omissions caused by the client or itself. In the case of an ARM, this can include reconciliations of a sample population of data submitted to the ARM by an investment firm or generated by the ARM on the investment firm's behalf with the corresponding data provided by the competent authority. The frequency and extent of such reconciliations should be proportionate to the volume of data handled by the ARM and the extent to which it is generating transaction reports from clients' data or passing on transaction reports completed by clients. In order to ensure timely reporting that is free of errors and omissions an ARM should continuously monitor the performance of its systems.

(15) Where an ARM itself causes an error or omission, it should correct this information without delay as well as notify the competent authority of its home Member State and any competent authority to which it submits reports of the error or omission as those competent authorities have an interest in the quality of the data being submitted to them. The ARM should also notify its client of the error or omission and provide updated information to the client so that the client's internal records may be aligned with the information which the ARM has submitted to the competent authority on the client's behalf.

(16) APAs and CTPs should be able to delete and amend the information which they receive from an entity providing them with information to deal with situations where in exceptional circumstances the reporting entity is experiencing technical difficulties and cannot delete or amend the information itself. However, APAs and CTPs should not otherwise be responsible for correcting information contained in published reports where the error or omission was attributable to the entity providing the information. This is due to the fact that APAs and CTPs cannot know with certainty whether a perceived error or omission is indeed incorrect since they were not party to the executed trade.

(17) To facilitate reliable communication between an APA and the investment firm reporting a trade, particularly in relation to cancellations and amendments of specific transactions, an APA should include in the confirmation messages to reporting investment firms the

***Changes to legislation:** There are outstanding changes not yet made to Commission Delegated Regulation (EU) 2017/571. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)EUR 2017 No. 571 may be subject to amendment by EU Exit Instruments made by the Financial Conduct Authority under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 1. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s. (See end of Document for details) View outstanding changes*

transaction identification code that has been assigned by the APA when making the information public.

(18) To comply with its reporting obligation under Regulation (EU) No 600/2014 of the European Parliament and of the Council[(2)], an ARM should ensure the smooth flow of information to and from a competent authority, including the ability to transfer reports and deal with rejected reports. The ARM should therefore be able to demonstrate that it can comply with the technical specifications set out by the competent authority regarding the interface between the ARM and the competent authority.

(19) A data reporting services provider should also ensure that it stores the transaction and trade reporting information which it handles for a sufficiently long period of time in order to facilitate the retrieval of historical information by competent authorities. In the specific case of APAs and CTPs, they should ensure that they establish the necessary organisational arrangements to maintain the data for at least the period specified in Regulation (EU) No 600/2014 and are able to respond to any request to provide services regulated by this Regulation.

(20) This Regulation sets out a number of additional services a CTP could perform which increase the efficiency of the market. In view of possible market developments, it is not appropriate to provide an exhaustive list of additional services which a CTP could perform. A CTP should therefore be able to provide further services going beyond the additional services specifically listed in this Regulation provided however that those other services do not pose any risk to the independence of the CTP or the quality of the consolidated tape.

(21) In order to ensure efficient dissemination of information made public by APAs and CTPs and an easy access and use of such information by market participants, the information should be published in a machine readable format through robust channels allowing for automatic access to the data. While websites may not always offer an architecture that is robust and scalable enough and that allows for easy automatic access to data, these technological constraints may be overcome in the future. A particular technology should therefore not be prescribed, but criteria should be set out that need to be met by the technology which is to be used.

(22) With respect to equity and equity-like instruments, Regulation (EU) No 600/2014 does not exclude that investment firms make public their transactions through more than one APA. However, a specific arrangement should be in place to enable interested parties consolidating the trade information from various APAs, in particular CTPs, to identify such potential duplicate trades as otherwise the same trade might be consolidated several times, and published repeatedly by the CTPs. This would undermine the quality and usefulness of the consolidated tape.

(23) When publishing a transaction, APAs should therefore publish transactions reported by investment firms by including a 'reprint' field indicating whether a report is a duplicate. In order to allow for an approach that is neutral in terms of the technology used it is necessary to provide for different possible ways in which an APA can identify duplicates.