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.

(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.

[1] OJ L 173, 12.6.2014, p. 349.

(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 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 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 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 ([1]), 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.

([1]) Regulation (EU) No 600/2014 of the European Parliament and of the Council on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

(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.

(24) In order to ensure that each transaction is only included once in the consolidated tape and therefore to strengthen the reliability of the provided information, CTPs should not publish information in relation to a transaction published by an APA which is identified as duplicative.

(25) APAs should publish information on transactions, including the relevant time stamps, such as the time when transactions were executed and the time transactions were reported. Furthermore, the granularity of the time stamps should reflect the nature of the trading system on which the transaction was executed. A greater granularity should be provided when publishing information on transactions executed in electronic systems than on transactions executed in non-electronic systems.

(26) CTPs may publish information on equity and non-equity instruments. Given the different requirements for the operation of those tapes, and in particular the significantly broader scope of financial instruments covered for non-equity instruments and the deferred application of the provisions of Directive 2014/65/EU for the non-equity consolidated tape, this Regulation only specifies the scope of the CTP consolidating information on equity-instruments.

(27) The provisions in this Regulation are closely linked, since they deal with the authorisation, organisational requirements and the publication of transactions for data reporting services providers. To ensure coherence between those provisions, which should enter into force at the same time, and to facilitate a comprehensive view by stakeholders and, in particular those subject to the obligations, it is necessary to include these regulatory technical standards in a single Regulation.

(28) This Regulation specifies the data publication requirements applicable to APAs and CTPs. In order to ensure consistent practices for publishing trade information across trading venues, APAs and CTPs and to facilitate the consolidation of data by CTPs, this Regulation should apply in conjunction with Commission Delegated Regulations (EU) 2017/587 ([1]) and (EU) 2017/583 ([2]) where detailed requirements applicable to the publication of trade information are set out.

(29) For reasons of consistency and in order to ensure the smooth functioning of the financial markets, it is necessary that the provisions laid down in this Regulation and the related national provisions transposing Directive 2014/65/EU apply from the same date. As Article 65(2) of Directive 2014/65/EU applies from 3 September of the year after the year of entry into application of this Regulation, certain provisions of this Regulation should apply from that later date.

(30) This Regulation is based on the draft regulatory technical standards submitted by the European Securities and Markets Authority (ESMA) to the Commission.

(31) ESMA has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the opinion of the Securities and Markets Stakeholder Group established by Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council ([3]),

HAS ADOPTED THIS REGULATION:

CHAPTER I

AUTHORISATION

(Article 61(2) of Directive 2014/65/EU)

Article 1

Information to competent authorities

1. An applicant seeking authorisation to provide data reporting services shall submit to the competent authority the information set out in Articles 2, 3 and 4 and the information regarding all the organisational requirements set out in Chapters II and III.

2. A data reporting services provider shall promptly inform the competent authority of its home Member State of any material change to the information provided at the time of the authorisation and thereafter.

Article 2

Information on the organisation

1. An applicant seeking authorisation to provide data reporting services shall include in its application for authorisation a programme of operations referred to in Article 61(2) of Directive 2014/65/EU. The programme of operations shall include the following information:

(a) information on the organisational structure of the applicant, including an organisational chart and a description of the human, technical and legal resources allocated to its business activities;

([1]) Commission Delegated Regulation (EU) 2017/587 of 14 July 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council on markets in financial instruments with regard to regulatory technical standards on transparency requirements for trading venues and investment firms in respect of shares, depositary receipts, exchange-traded funds, certificates and other similar financial instruments and on transaction execution obligations in respect of certain shares on a trading venue or by a systematic internaliser (see page 387 of this Official Journal).

([2]) Commission Delegated Regulation (EU) 2017/583 of 14 July 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council on markets in financial instruments with regard to regulatory technical standards on transparency requirements for trading venues and investment firms in respect of bonds, structured finance products, emission allowances and derivatives (see page 229 of this Official Journal).

([3]) Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

(b) information on the compliance policies and procedures of the data reporting services provider, including:

(i) the name of the person or persons responsible for the approval and maintenance of those policies;

(ii) the arrangements to monitor and enforce the compliance policies and procedures;

(iii) the measures to be undertaken in the event of a breach which may result in a failure to meet the conditions for initial authorisation;

(iv) a description of the procedure for reporting to the competent authority any breach which may result in a failure to meet the conditions for initial authorisation;

(c) a list of all outsourced functions and resources allocated to the control of the outsourced functions;

2. A data reporting services provider offering services other than data reporting services shall describe those services in the organisational chart.

Article 3

Corporate governance

1. An applicant seeking authorisation to provide data reporting services shall include in its application for authorisation information on the internal corporate governance policies and the procedures which govern its management body, senior management, and, where established, committees.

2. The information set out in paragraph 1 shall include:

(a) a description of the processes for selection, appointment, performance evaluation and removal of senior management and members of the management body;

(b) a description of the reporting lines and the frequency of reporting to the senior management and the management body;

(c) a description of the policies and procedures on access to documents by members of the management body.

Article 4

Information on the members of the management body

1. An applicant seeking authorisation to provide data reporting services shall include in its application for authorisation the following information in respect of each member of the management body:

(a) name, date and place of birth, personal national identification number or an equivalent thereof, address and contact details;

(b) the position for which the person is or will be appointed;

(c) a curriculum vitae evidencing sufficient experience and knowledge to adequately perform the responsibilities;

(d) criminal records, notably through an official certificate, or, where such a document is not available in the relevant Member State, a self-declaration of good repute and the authorisation to the competent authority to inquire whether the member has been convicted of any criminal offence in connection with the provision of financial or data services or in relation to acts of fraud or embezzlement;

(e) a self-declaration of good repute and the authorisation to the competent authority to inquire whether the member:

(i) has been subject to an adverse decision in any proceedings of a disciplinary nature brought by a regulatory authority or government body or is the subject of any such proceedings which are not concluded;

(ii) has been subject to an adverse judicial finding in civil proceedings before a court in connection with the provision of financial or data services, or for misconduct or fraud in the management of a business;

(iii) has been part of the management body of an undertaking which was subject to an adverse decision or penalty by a regulatory authority or whose registration or authorisation was withdrawn by a regulatory authority;

(iv) has been refused the right to carry on activities which require registration or authorisation by a regulatory authority;

(v) has been part of the management body of an undertaking which has gone into insolvency or liquidation while the person held such position or within a year after which the person ceased to hold such position;

(vi) has been otherwise fined, suspended, disqualified, or been subject to any other sanction in relation to fraud, embezzlement or in connection with the provision of financial or data services, by a professional body;

(vii) has been disqualified from acting as a director, disqualified from acting in any managerial capacity, dismissed from employment or other appointment in an undertaking as a consequence of misconduct or malpractice;

(f) An indication of the minimum time that is to be devoted to the performance of the person's functions within the data reporting services provider;

(g) a declaration of any potential conflicts of interest that may exist or arise in performing the duties and how those conflicts are managed.

CHAPTER II

ORGANISATIONAL REQUIREMENTS

(Article 64(3), (4) and (5), Article 65(4), (5) and (6), and Article 66(2), (3) and (4) of Directive 2014/65/EU)

Article 5

Conflicts of interest

1. A data reporting services provider shall 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 shall include policies and procedures for identifying, managing and disclosing existing and potential conflicts of interest and shall 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;

(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;

(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 as referred to in paragraph 1(a) shall 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 interest of another client or group of clients rather than the interests of a client to whom the service is provided;

(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.

Article 6

Organisational requirements regarding outsourcing

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 shall 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 shall 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 shall 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 shall remain responsible for any outsourced activity and shall 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;

(d) adequate business continuity of outsourced activities;

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

5. A data reporting services provider shall ensure that the third party service provider cooperates with the competent authority of the data reporting services provider in connection with outsourced activities.

6. Where a data reporting services provider outsources any critical function, it shall provide the competent authority of its home Member State with:

(a) the identification of the third party service provider;

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

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

For the purpose of the first sub paragraph 6, a function shall 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 Directive 2014/65/EU.

Article 7

Business continuity and back-up facilities

1. A data reporting services provider shall use systems and facilities that are appropriate and robust enough to ensure continuity and regularity in the performance of the services provided referred to in Directive 2014/65/EU.

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

3. A data reporting services provider shall 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 or 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 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;

(e) 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 shall be as short as possible and in any case no longer than six 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);

(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 shall set up a programme for periodically testing, reviewing and, where needed, modifying the business continuity arrangements.

5. A data reporting services provider shall publish on its website and promptly inform the competent authority of its home Member State and its clients of any service interruptions or connection disruptions as well as the time estimated to resume a regular service.

6. In the case of ARMs, the notifications referred to in paragraph 5 shall also be made to any competent authority to whom the ARM submits transaction reports.

Article 8

Testing and capacity

1. A data reporting services provider shall 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;

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

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

3. A data reporting services provider shall promptly notify the competent authority of its home Member State of any planned significant changes to the IT system prior to their implementation.

4. In the case of ARMs, the notifications referred to in paragraph 3 shall also be made to any competent authority to whom the ARM submits transaction reports.

5. A data reporting services provider shall set up an on-going programme for periodically reviewing and, where needed, modifying the development and testing methodologies.

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

7. A data reporting services provider shall:

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

(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.

Article 9

Security

1. A data reporting services provider shall 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 the information systems as defined in Article 2(a) of Directive 2013/40/EU of the European Parliament and of the Council [1];

(c) prevent unauthorised disclosure of confidential information;

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

2. Where an investment firm ('reporting firm') uses a third party ('submitting firm') to submit information to an ARM on its behalf, an ARM shall 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 via another submitting firm.

3. A data reporting services provider shall set up and maintain measures and arrangements to promptly identify and manage the risks identified in paragraph 1.

4. In respect of breaches in the physical and electronic security measures referred to in paragraphs 1, 2 and 3, a data reporting services provider shall promptly notify:

(a) the competent authority of its home Member State 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;

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

[1] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

5. In the case of ARMs, the notification referred to in paragraph 4(a) shall also be made to any other competent authorities to whom the ARM submits transaction reports.

Article 10

Management of incomplete or potentially erroneous information by APAs and CTPs

1. APAs and CTPs shall set up and maintain appropriate arrangements to ensure that they accurately publish the trade reports received from investment firms and, in the case of CTPs, from trading venues and APAs, without themselves introducing any errors or omitting information and shall correct information where they have themselves caused the error or omission.

2. APAs and CTPs shall 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 and CTPs shall perform periodic reconciliations between the trade reports they receive and the trade reports that they publish, verifying the correct publication of the information.

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

5. An APA shall 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 shall 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;

(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 shall not publish that trade report and shall promptly alert the investment firm submitting the trade report.

7. In exceptional circumstances APAs and CTPs shall delete and amend information in a trade report upon request from the entity providing the information when that entity cannot delete or amend its own information for technical reasons.

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

Article 11

Management of incomplete or potentially erroneous information by ARMs

1. An ARM shall set up and maintain appropriate arrangements to identify transaction reports that are incomplete or contain obvious errors caused by clients. An ARM shall perform validation of the transaction reports against the requirements established under Article 26 of Regulation (EU) No 600/2014 for field, format and content of fields in accordance with Table 1 of Annex I to Commission Delegated Regulation (EU) 2017/590 ([1]).

([1]) Commission Delegated Regulation (EU) 2017/590 of 28 July 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the reporting of transactions to competent authorities (see page 449 of this Official Journal).

2. An ARM shall 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 shall perform validation for field, format and content of fields in accordance with Table 1 of Annex I to Delegated Regulation (EU) 2017/590.

3. An ARM shall continuously monitor in real-time the performance of its systems ensuring that a transaction report it has received has been successfully reported to the competent authority in accordance with Article 26 of Regulation (EU) No 600/2014.

4. An ARM shall perform periodic reconciliations at the request of the competent authority of its home Member State or the competent authority to whom the ARM submits transaction reports between the information that the ARM receives from its client or generates on the client's behalf for transaction reporting purposes and data samples of the information provided by the competent authority.

5. Any corrections, including cancellations or amendments of transaction reports, that are not correcting errors or omissions caused by an ARM, shall 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 shall 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 shall not submit that transaction report and shall promptly notify the 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 shall promptly submit a correct and complete report.

8. An ARM shall promptly notify the client of the details of the error or omission and provide an updated transaction report to the client. An ARM shall also promptly notify the competent authority of its home Member State and the competent authority to whom the ARM reported the transaction report about the error or omission.

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

Article 12

Connectivity of ARMs

1. An ARM shall have in place policies, arrangements and technical capabilities to comply with the technical specification for the submission of transaction reports required by the competent authority of its home Member State and by other competent authorities to whom the ARM sends transaction reports.

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

Article 13

Other services provided by CTPs

1. A CTP may provide the following additional services:

(a) provision of pre-trade transparency data;

(b) provision of historical data;

(c) provision of reference data;

(d) provision of research;

(e) processing, distribution and marketing of data and statistics on financial instruments, trading venues, and other market-related data;

(f) design, management, maintenance and marketing of software, hardware and networks in relation to the transmission of data and information.

2. A CTP may perform services other than those specified under paragraph 1 which increase the efficiency of the market, provided that such services do not create any risk affecting the quality of the consolidated tape or the independence of the CTP that cannot be adequately prevented or mitigated.

CHAPTER III

PUBLICATION ARRANGEMENTS

(Article 64(1) and (2) and Article 65(1) of Directive 2014/65/EU)

Article 14

Machine readability

1. APAs and CTPs shall publish the information which has to be made public in accordance with Articles 64(1) and 65(1) of Directive 2014/65/EU in a machine readable way.

2. CTPs shall publish the information which has to be made in accordance with Article 65(2) of Directive 2014/65/EU in a machine readable way.

3. Information shall only be considered 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 Article 8(7) 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;

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

For the purposes of point (a) of the first subparagraph, the electronic format shall be specified by free, non-proprietary and open standards.

4. For the purposes of paragraph 3(a), electronic format shall include the type of files or messages, the rules to identify them, and the name and data type of the fields they contain.

5. APAs and CTPs shall:

(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 point (a) at least three months before they come into effect, unless there is an urgent and duly justified need for changes in instructions to take effect more quickly;

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

Article 15

Scope of the consolidated tape for shares, depositary receipts, ETFs, certificates and other similar financial instruments

1. A CTP shall include in its electronic data stream data made public pursuant to Articles 6 and 20 of Regulation (EU) No 600/2014 relating to all financial instruments referred to in those Articles.

2. When a new APA or a new trading venue starts operating, a CTP shall include the data made public by that APA or trading venue in the electronic data stream of its consolidated tape as soon as possible, and in any case no later than six months after the start of the APA's or trading venue's operations.

Article 16

Identification of original and duplicative trade reports in shares, depositary receipts, ETFs, certificates and other similar financial instruments

1. Where an APA publishes a trade report which is a duplicate, it shall insert the code 'DUPL' in a reprint field to enable recipients of the data to differentiate between the original trade report and any duplicates of that report.

2. For the purposes of paragraph 1, an APA shall require each investment firm to comply with one of the following conditions:

(a) to certify that it only reports transactions in a particular financial instrument through that APA;

(b) to use an identification mechanism which flags one report as the original one ('ORGN'), and all other reports of the same transaction as duplicates ('DUPL').

Article 17

Publication of original reports in shares, depositary receipts, ETFs, certificates and other similar financial instruments

A CTP shall not consolidate trade reports with the code 'DUPL' in the reprint field.

Article 18

Details to be published by the APA

1. An APA shall 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 Delegated Regulation (EU) 2017/587 and, use the appropriate flags listed in Table 3 of Annex I to Delegated Regulation (EU) 2017/587;

(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 Delegated Regulation (EU) 2017/583 and use the appropriate flags listed in Table 2 of Annex II to Delegated Regulation (EU) 2017/583.

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

3. By way of derogation from paragraph 2, an APA that publishes information regarding a transaction executed on an electronic system shall include the date and time, up to the millisecond, of the publication of that transaction in its trade report.

4. For the purposes of paragraph 3, an 'electronic system' shall mean 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. Timestamps referred to in paragraphs 2 and 3 shall, 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.

Article 19

Non-discrimination

APA and CTPs shall ensure that the information which has to 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.

Article 20

Details to be published by the CTP

A CTP shall make public:

(a) for transactions executed in respect of shares, depositary receipts, ETFs, certificates and other similar financial instruments, the details of a transaction specified in Table 2 of Annex I to Delegated Regulation (EU) 2017/587 and use the appropriate flags listed in Table 3 of Annex I to Delegated Regulation (EU) 2017/587;

(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 Delegated Regulation (EU) 2017/583 and use the appropriate flags listed in Table 2 of Annex II to Delegated Regulation (EU) 2017/583.

Article 21

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in *the Official Journal of the European Union*.

It shall apply from the date that appears first in the second subparagraph of Article 93(1) of Directive 2014/65/EU.

However, Articles 14(2) and 20(b) shall apply from the first day of the ninth month following the date of application of Directive 2014/65/EU.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 2 June 2016.

For the Commission
The President
Jean-Claude JUNCKER