►**B**

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)

(OJ L 87, 31.3.2017, p. 126)

Amended by:

		Official Journal		
		No	page	date
►**M1**	Commission Delegated Regulation (EU) 2018/63 of 26 September 2017	L 12	2	17.1.2018

▼B

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)

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;

(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;

▼B

(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;

▼B

(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.

▼B

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

(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;

▼B

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

(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

(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

(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.

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.

([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).

▼B

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.

▼B

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]).

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.

([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).

▼B

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.

▼B

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

(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.

▼M1

Article 15a

Scope of the consolidated tape for bonds, structured finance products, emission allowances and derivatives

1. A CTP shall include in its electronic data stream the data of one or more of the following asset classes:

(a) bonds, excluding exchange traded commodities (ETCs) and exchange traded notes (ETNs);

(b) ETC and ETNs bond types;

(c) structured finance products;

(d) securitised derivatives;

(e) interest rate derivatives;

(f) foreign exchange derivatives;

(g) equity derivatives;

(h) commodity derivatives;

(i) credit derivatives;

▼**M1**

(j) contracts for differences;

(k) C10 derivatives;

(l) emission allowance derivatives;

(m) emission allowances.

2. A CTP shall include in its electronic data stream the data made public pursuant to Articles 10 and 21 of Regulation (EU) No 600/2014 that meet both of the following coverage ratios:

(a) the number of transactions published by a CTP in an asset class listed in paragraph 1 represents at least 80 % of the total number of transactions in the relevant asset class published in the Union by all APAs and all trading venues during the assessment period referred to in paragraph 3;

(b) the volume of transactions published by a CTP in an asset class listed in paragraph 1 represents at least 80 % of the total volume of transactions in the relevant asset class published in the Union by all APAs and all trading venues during the assessment period referred to in paragraph 3.

For the purposes of point (b), the volume of transactions shall be determined in accordance with the measure of volume specified in Table 4 of Annex II to Commission Delegated Regulation (EU) 2017/583 ([1]).

3. A CTP shall assess the coverage ratios set out in paragraph 2 every six months, based on data covering the preceding 6 months. The assessment periods shall start on 1 January and 1 July each year. The first period shall cover the first six months of the year 2019.

4. A CTP shall ensure that it reaches the minimum coverage ratios set out in paragraph 2 as soon as possible, and in any case not later than:

(a) 31 January of the calendar year following the period covering 1 January to 30 June;

(b) 31 July of the calendar year following the period covering 1 July to 31 December.

([1]) 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 (OJ L 87, 31.3.2017, p. 229).

▼B

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.

▼B

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.

▼M1

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 3 January 2018.

However, Article 15a(4) shall apply from 1 January 2019 and Articles 14(2), 15(1), (2) and (3), and 20(b) shall apply from 3 September 2019.

▼B

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