

European Securities and Markets Authority
CS 60747
103 rue de Grenelle
75345 Paris Cedex 07, France
www.esma.europa.eu

CSA Partners 27.01.2014-3/2/25

Comments to Discussion Paper ESMA/2013/1649/ on ESMA's policy orientations on possible implementing measures under the Market Abuse Regulation

CSA Partners (CSA) provides market abuse compliance solutions to issuers of Nordic and Baltic Markets. Our mission is to simplify and increase the quality of compliance with the applicable Market Abuse regime.

Our offering, special purpose software (INSIDeR¹) designed for maintaining lists of insiders, ensuring the control of inside information and preventing illegal insider trading, is used by growing number of leading companies in the region for more than a decade.

We are grateful for the opportunity to share our long term regional experience and based on that provide observations and comments on discussion paper with respect to suggestions and questions contemplated by ESMA with respect to insider lists and related topics of compliance management.

I General observations and suggestions

Our experience of developing and implementing insider and inside information management solutions to Nordic and Baltic issuers confirms that national differences exist and indeed cause extra costs and administrative burden.

Regional interpretation of the term "insider list(s)" means either (i) list of corporate insiders (*individuals and entities assumed to have access to inside information on permanent or regular basis, including persons discharging managerial responsibilities*) or (ii) project specific insider list(s), the latter also referred to as logbook.

Administrative burden is particularly relevant in relation to obligations established with respect to corporate insiders. For instance some competent authorities have established special purpose declaration forms² that need to be signed and filed by the company (*e.g. form 501*) about corporate insiders (*e.g. form 501A*) and by such corporate insiders themselves. While the aim and purpose is understandable (*increase transparency, improve*

¹ Visit <http://www.csapartners.eu/insider-issuer-edition/> for further information.

² In case of Finansinspektionen these include "Company notification of insider position", "Company report of persons holding insider positions", "Report of holdings - at the time the insider position arose", "Report of changes in holdings - insiders and closely affiliated persons" etc, please see: <http://www.fi.se/Folder-EN/Startpage/Reporting/Insider-trading/Forms-for-insider-reporting/>

collection of data and its quality for market surveillance purposes) it does in fact impose substantial burden to issuers and individuals concerned. Such information collection would be substantially less burdensome if data could be submitted *per* agreed file or other output format directly from issuers' own internal compliance records management system.

Thus this is particular area where harmonisation and recognition of modern data exchange methods (*STP versus paper based forms*) could result in significant reduction of administrative burden to all stakeholders, including competent authorities who could reduce manual work.

The same cannot be said about logbooks: regulators and in some instances market operators (e.g. NASDAQ OMX Helsinki) in the Nordic-Baltic region have designed broadly similar framework and understanding with respect to logbooks:

- Entries of the logbook are meant to enable control and reconstruction of the flow of particular inside information (*i.e. who and when become exposed to inside information*).
- From the market integrity and investor protection perspective it is the logbook (*not the list of corporate insiders*) which is viewed as primary tool for maintaining and verifying confidentiality obligations with respect to undisclosed inside information.
- Individual logbook (*versus list of corporate insiders*) is the primary instrument for competent authorities in the case of suspicious trading patterns referring to leaks ahead of disclosure.
- Updating of the logbook must be made without delay (*at the latest on the same day*).
- Person entered to the logbook needs to be informed in writing or other verifiable manner (*e.g. via e-mail*) about the fact and implications of being entered in the logbook and being in possession of price sensitive information. Reason is obvious - to ensure that person understands the legal meaning of his situation that among other things means (i) no trading, (ii) no leaks and (iii) no hints as each of the foregoing constitutes offence.
- Each individual logbook shall be saved for at least five years after it was drawn up or after the date when it was last updated.
- Data components of the logbook derive from the assumption that logbook should in principle enable reasonably precise reconstruction of the flow of specific inside information case (*even among corporate insiders*) and are in general as follows:
 - Description of the case: usually based on code-names to avoid incidental leaks;

- Identity of the recipients: name, surname, personal identification number, position, address and or e-mail address of the persons who was involved to the case;
- Date and time: when person in the logbook received inside information in question;
- Information source and circumstances: who provided information to the recipient and on what circumstances (*meeting, telco etc*);
- Reason: brief explanation or justification of a reason why was recipient exposed to inside information (*e.g. employment duties*).

Considering the above we suggest ESMA to work towards the following framework that in our opinion would (i) reduce unnecessary administrative burden on issuers and corporate insiders from one hand and (ii) maintain clear and simple rules when it comes to the requirement to control the flow of inside information and be able to assist competent authorities with reasonably precise reconstruction of it:

- There are unified and proportional rules on maintenance, data content and other aspects when it comes to the list of **corporate insiders** (*permanent insiders if you wish*).
- Competent authorities' rights vis-à-vis issuers on data collection about corporate insiders should be harmonised as follows:
 - Local competent authorities should not be entitled to introduce or continue local paper-based declaration requirements towards corporate insiders as the only channel for submission of data as this poses onerous administrative burden, especially for issuers whose management team members come from or are located across different Member States;
 - As an alternative to paper-based data collection local competent authorities should provide the possibility for transmission, including regular transmission (*e.g. in case there is a change*) of data about the list of corporate insiders and associated persons of PDRMS³ - thus competent authorities shall maintain or even improve the possibility of feeding their internal market monitoring databases.
- We suggest the following data components when it comes **to the list of corporate insiders**:

³ Persons discharging managerial responsibilities.

- **Date and time:** mandatory, reflecting date and time when the extract or report of the list is made;
- **Forename and Surname** - mandatory, self-explanatory;
- **Personal ID** - mandatory, national social security code, employee number or similar code should be acceptable if that enables the issuer to ensure that conclusive identity of the person can be provided to the competent authority upon request;
- **E-mail:** optional, provided that issuer is able to provide this upon further request;
- **Contact Address:** optional, provided that issuer is able to provide this upon further request;
- **Contact Phone:** optional, provided that issuer is able to provide this upon further request;
- **Employer and position (function):** mandatory, self-explanatory;
- **Permanent access start date:** mandatory, self-explanatory;
- **Explanation:** optional informative field to describe the reasons why was person included to the list of permanent insiders;
- **Permanent access end date:** mandatory if applicable, self-explanatory;
- **PDRMS start date**⁴: mandatory if applicable (i.e. status "Persons discharging managerial responsibilities" is applicable);
- **Explanation:** optional informative field to describe the reasons why was person included to the list of PDMRs;
- **PDRMS end date:** mandatory if applicable;
- **Date and time of the last update:** optional, provided that issuer is able to provide it upon further request (*modern compliance records management systems include audit trail feature*).

Above approach - i.e. leaving some fields optional - recognises that primary source of personal, contact or other relevant data about corporate insider may actually be in other internal (e.g. HR) database or system(s). Issuer can perform extra reconciliation of insiders' personal and contact data against primary database or system upon "if needed" follow-up request from the competent authority. Recognising this by ESMA would optimise issuers' personal data processing and maintenance obligations and thus reduce unnecessary administrative burden.

Such approach is also justified given that correctness of the data becomes more critical due to substantial increase of maximum administrative pecuniary sanctions: EUR 500 000 for natural person and EUR 1 000 000 for legal persons for breaches relating to insider lists.

⁴ There is a practical but also regulatory need for the purposes of compliance management to differentiate permanent insiders from those that have also the status of PDMR since not every permanent insider is automatically PDMR. To achieve the compliance with the requirement of Article 14 1 that reads as follows: "1d. Issuers shall notify the persons discharging managerial responsibilities within that issuer of their obligations under this article in writing. Issuers shall draw up a list of all persons discharging managerial responsibilities and persons closely associated with them. Persons discharging managerial responsibilities within an issuer shall notify the persons closely associated with them of their obligations under this article in writing and shall keep a copy of this notification."

- There are unified and proportional rules on maintenance, data content and other aspects when it comes to logbooks. **Note that logbook format shall be used by both by issuers as well as by parties performing the tasks for the issuer.** We suggest the following data components when it comes **to the logbooks:**
 - **Date and time:** mandatory, reflecting date and time when the extract or report of the list is made;
 - **Project name** - mandatory, self-explanatory, use of code names should be encouraged to avoid accidental leaks;
 - **Forename and Surname** - mandatory, self-explanatory;
 - **Personal ID or Registry Code** - mandatory, national social security code, employee number or similar code should be acceptable in case of natural persons if that enables the issuer to ensure that conclusive identity of the person can be provided to the competent authority upon request. Registry code of the legal person should also be the possibility;
 - **E-mail:** optional, provided that issuer is able to provide it upon further request;
 - **Contact Address:** optional, provided that issuer is able to provide it upon further request;
 - **Employer and position:** optional, provided that issuer is able to provide it upon further request;
 - **Date and time when access was obtained:** mandatory, self-explanatory, with the precision-level of hours at least;
 - **Source and circumstances:** optional, provided that issuer is able to provide it upon further request. The purpose is to be able to obtain information as to who and on what circumstances (*be it teleconference or physical board meeting*) provided the information;
 - **Explanation:** optional informative field to describe the justification (*e.g. employment duties*) of the selective disclosure, provided that issuer is able to provide it upon further request;
 - **Date and time of the last update:** optional, provided that issuer is able to provide it upon further request.

Here again we suggest certain fields to be left as optional provided that issuer has systems and controls in place to elaborate circumstances required in those fields upon further request. Having above mandatory fields as part of initial submission of logbook should enable competent authority to attend majority of their first-round supervisory duties. Above approach provides certainty and makes clear to both ends (*issuer and competent authority*) what is the information that competent authority may require should further proceedings require additional details.

II Responses to specific questions

Q84: Do you agree with the information about the relevant person in the insider list?

No. Please see our suggestions on data components of the list of corporate insiders and logbooks, including proposal to leave certain components optional.

As stated above we do not think that insider list(s) should be or become a database where issuers have to duplicate collection, storage and processing of personal data and especially (i) of the data which does not serve any purpose or (ii) which has been collected, is stored and maintained in other internal databases or IT systems of the issuer and can be reconciled from there in the event where competent authority becomes actually interested.

The following information represents a very clear case of (i) and should thus be left out:

- "Name of birth";
- "Date of birth",
- "Place of birth",
- Various telephone numbers (more than one).

Our proposal suggests leaving some fields optional - recognising that primary source of personal, contact or other relevant data about corporate insider is in other internal (*e.g. HR*) database or system(s). Issuer can perform extra reconciliation of insider's data against primary database or system upon "if needed" request from the competent authority. Recognising this by ESMA would optimise issuers' personal data processing and maintenance obligations and thus reduce unnecessary administrative burden.

Q85: Do you agree on the proposed harmonised format in Annex V?

First of all it seems that the text of the consultation paper does not match with Annex V in all respects (*thus giving rise to question as to whether the right version of Annex V has been attached*). We would like to highlight the following points that are either controversial or difficult to understand when looking at points 322 - 325 in combination with Annex V:

- Point 322 states the following: "*Regarding (c), the date on which the list of insiders was created and updated, the proposed format allows for the creation of one single consolidated list, which would be electronically created and stored. This would be constantly updated to reflect additions and removals. It is important that both the date of update and the specific change made be easily identifiable by the competent authority.*"

It is difficult to understand what exactly is expected from the issuers: in particular it remains unclear how exactly should issuers make changes easily identifiable by the competent authority? If person is deleted from the list then version of the file following that deletion does not reflect the person anymore.

We wonder if ESMA may mean making changes identifiable *via track changes* format? If so then we do not find this to be a reasonable solution neither for competent authorities nor for issuers. It will be difficult to handle, and problematic for STP. We predict that file of the average issuer would become incomprehensible rather sooner than later.

We have no good alternative in case of handling list in *MS Excel* but would like ESMA to recognise also the "database approach" which means that all corporate insider and logbook records are maintained in a database which enables "as of" backdate queries and reports and is supported by audit trail. In our opinion this is in fact the only way to properly meet 5-year storage requirement⁵ as this means that every version of the list (*or state of database following or preceding each update*) needs to be fully restorable 5 years after the update.

- Last sentence of 322 reads as follows: "*... Thus crucially, providing clear indication of the chronology of possession of inside information*"

We were unable to identify any field in Annex V that would assist in understanding the chronology of possession of inside information. Making asterisk behind person's data and under the project name may be useful in indicating that person in question is logbook insider for the project (*e.g. Project 1 where Aiden Connor seems to be involved*) but that does not offer any clue (*neither date nor time*) as to when did person became exposed to information. Such asterisk-based solution does not offer any chronological reconstruction opportunities with respect to information flow and thus fails to comply with Article 13 1b (c)⁶.

Adding format DD.MM.YYYY,HH:MM (e.g. 03.02.2014 15:30) - to reflect the time when access was obtained - instead of asterisk behind the person and under the particular project would partly rectify this (*using field obtained would fail in case the person in involved in more than one project at the same time*).

But even with this we foresee that consolidated list becomes very difficult to manage (*for the issuer*) and hard to follow (*for the competent authorities*) as soon as the number of insiders grows beyond 30 and number of projects beyond 4 (*depending on the size of the monitor and skills of Excel usage*). There would be also problem with finding the place for "access ceased" in the context of specific project.

The number of active simultaneous price sensitive projects varies issuer by issuer. We have examples of large financial sector issuer that had around 50 projects in progress at the same time. Let alone old projects which due to 5 year-storage rule

⁵ "1d. The insider list shall be retained by the issuers and any person acting on their behalf or account for a period of at least 5 years after being drawn up or updated."

⁶ Article 13 1b (c) "1b. The insider list shall include at least: (c) the date and time at which such person obtained access to inside information;"

and proposed approach should appear in the list, thus accumulating the number of occupied columns to the extent that is impossible to manage. The only practical way in case of issuers with large number of projects is to maintain individual logbooks separately from the list of corporate insiders and each other.

- Point 323 states the following: *"Regarding (d), the date and time at which such person obtained inside information and (e) the date and time at which such person ceased to have access to inside information, these are priority fields which require the inclusion of specified dates and times in an insider list. When recording time, it is proposed that the relevant time zone should be specified (for example CET or GMT)."*

Even though it is not clear per sample filling (*there are neither hours, minutes nor references to time-zone*) we understand that value of column "Obtained" should refer to exact time and zone specification of the moment when person in question was exposed or involved to the specific project. If our understanding is correct then we would see a structural problem in case the person is involved in more than 1 project with different "access times" at the same time (*this being very common in reality*)?

In conclusion we doubt if ESMA should come up with the sample format of single document-based (consolidated) approach since this is too complex and difficult to manage (*by issuers*) and comprehend (*by competent authorities*) in real life. Introducing a complex and poor (*in terms of practical application*) format as a primary layout for the issuers and third parties would carry the risk of substantial working accident from the perspective of competent authorities because they will have to face the result, including different interpretations, varying levels of MS Excel usage etc. Keeping things as simple as possible is the best approach here.

For the above reasons and the fact that majority third-parties like advisors, accountants and credit rating agencies, would be expected to keep only logbook type of lists - we suggest ESMA to consider the following options:

- a) Introduce separate (from the logbook) format with data components suggested under "*I General observations and suggestions*" for corporate insiders. This is to be used primarily by the issuers. The main function of this type of list is to manage and keep track of individuals with permanent and / or regular access to inside information, PDMRs and if so desired by the issuer, for compliance management and prevention purposes in the context of Article 14, also associated persons of PDMRs;**
- b) Introduce separate format with data components suggested under "*I General observations and suggestions*" for logbooks and permitting also submission of all logbooks on a consolidated sheet – to be used by issuers as well as by third parties such as advisers, accountants or law firms working for issuer on specific**

matter(s). The main function of this type of list is to keep track of the flow of specific inside information and meet the requirements of Article 13 1b (c).

ESMA could of course consider once more if there is a good way to continue with Annex V-type of consolidated approach. If it succeeds in finding a solution that is manageable under real life conditions (*multiple simultaneous cases, old cases, number of insiders between 20 – 100*), then introduce this as one alternative to simplified "separated lists" approach (*a and b above*) that might be useful for companies with only recent listing or issuers that have smaller number of insiders and rare occasions of logbook events due to nature of their business.

Any and all format(s) introduced by ESMA should be without prejudice to the issuer's right to adopting a different methodology as long as requirements of the data content and reliability of maintenance are met.

Q86: Do you agree on the proposal on the language of the insider list?

Yes, this is reasonable and to large extent reflects today's reality.

Q87: Do you agree on the standards for submission? What kind of acceptable electronic formats should be incorporated?

Proper use code names when denoting log-book projects would turn individual logbook into information asset with relatively low vulnerability rating (*except for concern of the leak of personal data which would be mitigated if ESMA would accept certain fields as optional per our suggestions above*). Thus cases and situations may differ and it may be acceptable for individual logbook to be delivered to competent authority without encryption. Might be that it is most appropriate to leave this matter to the discretion of the issuer.

Q88: Should ESMA provide a technical format for the insider list including the necessary technical details about the information to be provided (e.g. standards to use, length of the information fields...)?

Yes, we recommend this to be available as an option (*versus obligatory*) to the benefit of issuers. This option should be available to issuers as an alternative to any signed local document-form or declaration template if competent authorities are permitted to maintain them.

Issuers should have the right to request that instead of signed forms data can also be provided *per* data exchange formats (*e.g. XML, CSV, MS Excel*) customary to modern information exchange arrangements.

That would provide issuers with the possibility to optimise internal compliance management in modern, safe and convenient manner towards all parties involved. Modern compliance management systems would support provision of data to competent authorities *via* STP

and thus in this way reduce also competent authorities' workload (*re-entering the data from paper forms*).

Q89: Do you agree on the procedure for updating insider lists?

Section 329 states what is already obvious (*list is to be maintained by the issuer or ... and that it has to be available for 5 years*) and does not seem to say much about the requirements that should apply to basic aspects of updating procedures in view of ensuring reliability of data. We recommend ESMA to revisit this with more thorough focus on the following basic aspects and questions:

- Time limits of the update to clarify the meaning of "promptly update" in Article 13? We would recommend "without undue delay but at the latest within the same day when the underlying circumstance or event materialized (*e.g. new persons were involved into the project*)".
- Does "electronic document" encompass also special purpose electronic database?
- What are the acceptable ways to meet "*Each update shall specify the date and time when the change triggering the update occurred.*" in Article 13? Is audit trail - showing who of the users updates the field and what was the change - of updates good enough to meet this?
- Should the manner of maintaining and updating the list permit to identify who has done the update (*we consider this to be basic and reasonable requirement*)?
- Should issuers take measures to avoid unauthorised access and updates (*at least some high level requirements*)?

Q90: Do you agree on the proposal to put in place an internal system/process whereby the relevant information is recorded and available to facilitate the effective fulfilment of the requirement, or do you see other possibilities to fulfil the obligation?

Yes, there seems to be no better alternative. We recommend this to be applicable - as a general requirement – to all issuers, not only to SME Growth Market issuers.

Q91: Are these characteristics sufficiently clear? Or are there other characteristics which must be shared by all transactions?

Yes they are sufficiently clear.

Q92: What are your views on the minimal weight that the issuer's financial instrument should have for the notification requirement to be applicable? What could be such a minimal weight?

We think this to be reasonable direction but have no additional suggestions at this stage.

Q93: For the avoidance of doubt, do you see additional types of transactions that should be mentioned to the non-exhaustive of examples of transactions that should be notified?

Not at this stage.

Q94: What are your views on the possibility to aggregate transaction data for public disclosure and the possible alternatives for the aggregation of data?

We do not support aggregation for the sake of transparency. Further, it is common that issuers' internal insider rules provide for minimum holding period which means that short term same day trading among PDMRs would be highly unusual.

Article 14 (1) requires PDMRs and their associates to notify the issuer and the competent authority about their transactions. We suggest that PDMRs and their associates' transactions can be notified to competent authorities also *via* issuers (*e.g. compliance function*) and once that is done, EU law (*via ESMA standards*) should consider PDMR or his associate's obligation discharged without any risk of sanction.

As regards format of notification from the issuer to competent authority, then electronic output *per* data format ordinary in the sphere of modern electronic communication should be possible as an alternative.

Q95: What are your views on the suggested approach in relation to exceptional circumstances under which an issuer may allow a PDMR to trade during a trading window?

From Article 14 it is not very clear if pre-approved share purchase plans with "stop-loss" order vehicles would also be permitted. In our opinion this is necessary in order to avoid that certain Member States rule closed periods as such to be unconstitutional. Likelihood of this happening is lower if person can take protective measures for saving value of his assets.

Respectfully,



Martin Villig
Chairman of the Board
Martin.Villig@csapartners.eu
www.csapartners.eu