1 April 2024

To: The Management Body,

To: The Compliance Officer,

Thematic Review on Governance and the Compliance Function in relation to Trustees and Company Service Providers

You are receiving this letter as the Management Body and/or Compliance Officer and/or the person responsible for the Compliance function (the "Compliance Officer") of a Trustee[1] or Company Service Provider ("Authorised Person") supervised by the Malta Financial Services Authority (the "MFSA" or "Authority").

BACKGROUND AND METHODOLOGY

In order for the Authority, as the single regulator of financial services, to be in a position to supervise effectively, a thorough understanding of the sector, current and emerging risks and the respective business models of authorised persons, is essential.

A thematic review is one of the ways in which this can be achieved, as it is in fact an effective supervisory tool utilised by regulatory authorities in various jurisdictions, which enables them to focus supervisory efforts on specific areas of concerns (themes) across a group of regulated entities, analysing common issues, risks, or practices, as opposed to focusing on a single authorised person. Moreover, the publication of the findings of a thematic review renders this supervisory tool even more effective. It promotes transparency through the sharing of findings and insights with the industry and the public, which in turn fosters trust and confidence in regulatory processes. Furthermore, it also holds regulated persons accountable for their actions and practices by highlighting areas needing improvement and encourages regulated persons to address deficiencies promptly. By raising awareness on common issues, risks or emerging trends, thematic reviews provide benchmarks for all authorised persons to assess their own practices against industry norms and regulatory expectations. Thematic reviews also promote continuous improvement for regulated persons, and equally for regulators, through the assessment of industry practices and regulatory compliance, enabling stakeholders to identify areas for enhancement and implement necessary changes to improve overall outcomes.

[1] Reference to 'Trustee' or 'Trustees' in this document should be interpreted as referring to any person authorised in terms of the Trusts and Trustees Act to provide the services of trustee, and/or other fiduciary services, including acting as mandatary or administrator of private interest foundations.

To this effect, the Trustees and Company Service Providers ('TCSPs') Supervision Function within the Authority has chosen to conduct part of its supervisory assessment for 2021- 2023 using this supervisory tool, as further detailed in this letter. The focus of this thematic review (the 'Review') revolved primarily around the assessment of the sector's Governance and the Compliance culture and the effectiveness thereof, in line with the MFSA's Supervision Priorities. The aim of this Review was to identify the current and emerging risks in these areas and to share with the sector the Authority's expectations in addressing the findings identified. The authorised persons forming part of this Review were chosen on the basis of the Authority's risk-based approach to supervision, which determines the frequency, focus and depth of supervisory engagement with authorised persons. The findings outlined in this document emanate from a sample of 19 supervisory interactions carried out between 2021-2023, making up 25.37% of the total supervisory interactions carried out by the TCSPs Function in this period. The 19 supervisory interactions were divided into 9 supervisory inspections and 10 supervisory meetings, accordingly.

The purpose of this letter is to inform the industry about the main findings of this Review, as well as to communicate the Authority's expectations, and to encourage authorised persons to take any necessary corrective action where gaps are identified. Overall, the Authority positively notes improvements in TCSPs' governance structures and compliance culture especially when compared to previous years. Through this Review, the Authority positively observed a willingness among TCSPs to enhance their governance and compliance tools and practices. A positive observation related to a notable increase in investment in compliance tools and resources and in systems to enhance controls, which strongly suggests that TCSPs are acknowledging the long-term benefits of identifying current and future risks. The Authority noted a strong increase in the importance given to ongoing training on various aspects of the business, undertaken by senior officials of authorised persons and their staff which in turn evidently increased the level of service. This Review highlights the areas where the sector needs to improve and underscores the need for TCSPs to take the necessary actions to align their business with the MFSA's expectations, and to implement sound and resilient governance and compliance practices, especially in the light of the publication of latest National Risk Assessment ("NRA") and the risks outlined therein vis-à-vis this sector. During the period underlying this Review, the CSP sector underwent a significant change. By virtue of the Company Service Providers (Amendment) Act, certain persons who were already providing CSP services (either as warranted professional or under the *de minimis* ruling) were brought under the MFSA's supervisory remit. Through the supervisory engagements, the Authority noted a general willingness and appetite of authorised persons to align their operations to the Authority's expectations.

While the sample is comprised exclusively of authorised legal persons, natural persons authorised in terms of the Trusts and Trustees Act (the 'TTA') or the Company Service Providers Act (the 'CSP Act') are nonetheless expected to review the Key Findings outlined below and ensure that, where appropriate, necessary action is taken to ensure they are in line with the Authority's expectations, whilst adapting the corrective action to the size, nature and complexity of the authorised person's set up in terms of the proportionality principles applied by the Authority.

KEY FINDINGS

1. Matters relating to Governance

1.1. The Board of Directors (the 'Board')

The Authority positively noted, through interviews carried out as part of this Review, that directors are generally involved and engage in discussions relating to key matters of entities' regulated business. However, the Authority noted that TCSPs often lacked the formality of retaining detailed minutes of such discussions.

From a review of Board meeting minutes provided, the Authority observed some instances where such minutes did not extend to discussions relating to the key matters impacting the authorised business, such as client onboarding, risk and compliance, and instead discussions appeared to be restricted to formal operational matters of the business. Consequently, the Authority was not in a position to assess whether other key strategic matters were in fact being discussed by the Board, nor assess the effectiveness of the Board in taking key decisions. In other cases, whilst Board meeting minutes did include reference to integral matters, the said minutes did not include sufficient detail on the discussions leading to decisions taken by the Board. In most cases, it was explained to the Authority that this was due to the fact that the directors often engaged in informal discussions relating to the authorised business which discussions were, however, not subsequently documented.

During the course of certain supervisory interactions, the Authority observed that certain Board members lacked a comprehensive understanding of the workings of key functions and processes of the Authorised Person. In one of these instances, the lack of involvement by certain members of the Board and the lack of, at least, a high-level understanding of key aspects of the business, was a result of having a dominant director on the Board. The Authority noted that in such instances, all decisions were being taken by the dominant director with the rest of the Board simply being informed of decisions taken, without the opportunity to discuss and possibly challenge such decisions, resulting in weak checks and balances and an ineffective Board.

The Authority also observed two instances where one Director held multiple other roles, such as also being the Company Secretary, and Compliance Officer and/or MLRO of the Authorised Person, and possibly also one of the shareholders, without implementing adequate mitigating measures and controls.

The Authority noted one instance where findings and breaches were communicated to the Board by both internal and external functions, such as the compliance function or external auditors, identifying weaknesses or even breaches, however no action or proper effective action was taken by the Board to remediate such findings. In this instance, the compliance officer advised the Board to ensure that Board minutes include sufficient detail of discussions held at Board level however, the Authority noted that months following this recommendation, this was not in fact implemented and adopted by the

Board. This also extends to implementing necessary mitigating measures for the avoidance of breaches resulting from administrative penalties imposed by other authorities or bodies.

Regulatory Requirements

In line with R3-6.6.3 of the Company Service Providers Rulebook[2] (the "CSP Rulebook") and Section 9.4 of the Trusts and Trustees Code of Conduct[3] (the "Trustees Code of Conduct"), Authorised Persons are reminded that they are required to maintain Board meeting minutes which provide a true and accurate record of discussions held, decisions taken, and resolutions made, especially those relating to significant and strategic matters concerning the authorised business. Where any key decisions are taken by Board members outside of formal Board Meetings, such decisions should be duly recorded in the form of resolutions. Board minutes and resolutions should enable external parties to understand Board discussions and decision-making processes, as set out in the Corporate Governance Code: Enhancing the Governance, Culture, and Conduct of MFSA Authorised Entities[4] (the "Corporate Governance Code") issued by the MFSA on 5 August 2022, and which all Authorised Persons are required to adhere to, on a best effort basis. In terms of good governance practices, adequate Board packs should also be retained, including any supporting documentation referred to in such minutes.

Authorised Persons are reminded that all the Directors of an Authorised Person are responsible for the general direction and strategy of the authorised business. Whilst Directors may be assigned specific roles within the business, all members of the Board are expected to have a general understanding of the workings of key functions and processes of the Authorised Person. Where a single individual is particularly dominant in an undertaking this will raise doubt about the effectiveness of the Board and the overall management of the authorised business.

Authorised Persons are further reminded of R3-6.2(vii) of the CSP Rulebook and Sections 9.4 and 6.0 of the Trustees Code of Conduct. It is imperative for TCSPs to ensure that structures where one person is holding multiple roles, do not give rise to any issues relating to, for example, time management and conflicts of interest. Such instances could also lead to an inappropriate application of the Three Lines Model, leading to a lack of organisational independence of the different functions and a lack of checks and balance within the structure of the Authorised Person. Where necessary, appropriate mitigating measures and controls are expected to be adopted by the Authorised Person.

Authorised Persons are reminded that the Board is expected to implement appropriate remediation strategies and mitigating measures in order to address findings identified or avoid repeated breaches and align the authorised business with applicable legislative and regulatory standards and obligations. Authorised Persons are also expected to ensure to document all action taken and mitigating measures adopted, accordingly.

[2] https://www.mfsa.mt/wp-content/uploads/2021/03/Company-Service-Providers-Rulebook.pdf
[3] https://www.mfsa.mt/wp-content/uploads/2019/01/Trusteescodeofconduct.pdf
[4] https://www.mfsa.mt/wp-content/uploads/2022/08/MFSA-Corporate-Governance-Code.pdf

1.2. Policies and Procedures

The Authority positively noted that all authorised persons forming part of this Review had in place policies and procedures in line with applicable legislative and regulatory frameworks. Some instances were noted where authorised persons did not have in place certain policies or procedures, including: (i) a governance policy outlining reporting lines and decision-making procedures; (ii) an outsourcing policy; (iii) compliance-related procedures; and/or (iv) cybersecurity policies/procedures.
In a few instances, authorised person's policies and procedures were found to be too high level and did not include the practical application of the relevant principles by the authorised persons in day-to-day operations. For instance, the governance policy did not include decision-making procedures, and fell short of extending to the specific responsibilities of the directors, reporting lines and the manner in which the authorised person applies the dual control principle. In other instances, the Business Continuity Plan did not include procedures to provide for the continuity of functions in circumstances of long periods of absence of any of the key officers of the Authorised Person, including the Directors and the Compliance Officer.

Inadequate policies and procedures, as well as weaknesses in the necessary controls to ensure adherence therewith, may reflect poor governance practices adopted by the authorised person, which may in turn lead to failures in other aspects of the business. For example, in some instances it was observed that where authorised persons had an inadequate Client Risk Assessment Policy in place, this resulted in the said authorised persons not carrying out client file reviews and ongoing monitoring in line with the review timeframes outlined in their respective Client Risk Assessment Policy. This could in turn expose the authorised person to unnecessary risks of failure to identify certain gaps, or indeed red flags during the business relationship.

Regulatory Requirements

Authorised Persons are reminded of R3-2.2, R3-6.2 - R3-6.4, R3-7.1, R3-8.1, R3-9.1, R3-10.1, R3-11.9.1 of the CSP Rulebook and Sections 9.4, 9.8 and 9.11 of the Trustees Code of Conduct. Furthermore, Authorised Persons are expected to ensure that policies and procedures are reviewed at least annually.

1.3. Client onboarding & Ongoing Monitoring

1.3.1. *Client Onboarding Decision-Making*

In two instances concerning medium-sized authorised persons, the Authority noted governance structures whereby the Board of Directors did not have the final determination in terms of client onboarding. The Authority noted that in these two instances, Senior Management was responsible for the client onboarding decisions and the Board was only being notified of new clients onboarded after onboarding had already taken place. In such instances, it was observed that although this practice was only applied to low risk clients, this was done without any formal written procedure in place. Moreover,

this also deviated from the operations as originally communicated to the Authority at authorisation stage, and without prior notification to, or approval by the Authority.

In three instances, the Authority noted that client onboarding was not being carried out in line with the dual control principle. For example, having only one Director, or the Money Laundering Reporting Officer alone, responsible for the final determination as to whether a client should be onboarded, or otherwise. Other instances included having persons not being approved persons by the Authority involved in the implementation of the dual control principle as applied to client onboarding.

Regulatory Requirements

Authorised Persons are reminded that at authorisation stage, the Authority approves the Board as the main decision-making body of the Authorised Person. Should any of the core functions of the Board be delegated to any other person, committee or body, the Authorised Person should obtain prior approval from the Authority for any intended changes to be made to the approved governance structure. Furthermore, in such instances the Authorised Person should also have in place a formal delegation framework clearly outlining this arrangement which should also be approved by the Authority. The Authority would like to emphasise that whilst it is acceptable and understandable for an Authorised Person to implement various operational arrangements which best address the size, nature and complexity of its business, the Board remains ultimately responsible for all key decisions, including client onboarding, irrespective of any such arrangements which may be in place.

Furthermore, authorised persons are referred to R3-6.6.2 – R3-6.6.4 of the CSP Rulebook and Section 5 of the Trustees Code of Conduct which set out the regulatory obligation of authorised persons to manage the business in accordance with the dual control principle. Therefore, in line with this principle, authorised persons set up as legal persons are required to ensure that all decisions relating to the regulated business, including client onboarding, are effectively taken by at least two directors or by a director and another senior official of the authorised person duly approved by the Authority. In the latter instances, prior approval by the Authority should be sought and following which, duly formalised in the authorised person's procedures.

1.3.2. *Client Agreements*

The Authority noted a few shortcomings in client agreements reviewed in terms of missing key elements, such as omitted reference to the specific licensable service/s being covered by the agreement. This resulted in difficulties in establishing the services provided to the client. The Authority further observed that in instances where a group of entities are servicing a common client, the common client agreement in place failed to specifically indicate the specific entity providing the respective licensable service, which may be misleading to the client, or even possibly raise concerns as to whether the licensable services are being provided through the duly authorised entity.

The Authority also observed a few instances where client agreements and/or letters of engagement were found to have deficiencies such as missing signatures for one or more parties to the agreement, or failure to identify the role of the signatory, as well as agreements not being duly dated.

Regulatory Requirements

Authorised Persons are requested to ensure that client agreements clearly outline the licensable services being provided and covered by the agreement, and in the case of a group of companies or related entities providing multiple services to the client, an indication as to which licensed entity is offering the respective licensable services. Should one entity within a group be formally authorised to sign client agreements for and on behalf the rest of the entities within the group, the necessary underlying agreements and/or resolutions should be in place. Authorised Persons are reminded of the applicable requirements in terms of R3-11.7.1 of the CSP Rulebook and Section 6.0 of the Trustees Code of Conduct, in this regard.

1.4. Resource Sharing & Outsourcing Agreements

The Authority observed on one occasion that an authorised person forming part of a group of companies shared resources and outsourced certain key functions to third parties, without having any underlying resource sharing and/or outsourcing agreements in place.

Regulatory Requirements

Authorised Persons are required to have in place the necessary underlying agreements governing sharing of resources or outsourcing of services. Such agreements are required to be set out in a formal, clear, written contract which establishes the respective rights and obligations of the parties. Reference is made to 'Title 9 Outsourcing' of the CSP Rulebook and Section 9.8 of the Trustees Code of Conduct.

1.5. Regulatory Registers

Through this Review, the Authority noted one instance where the Authorised Person did not have in place a risk register required by the applicable regulatory framework. In other instances, albeit having the relevant registers in place, the Authority noted a lack of certain key details recorded in such registers, such as in the complaints, conflicts of interests, risk, and/or breaches registers. Such omissions included, for example, a reference to the client in question when noting details in the complaints register and a description of the breach recorded in the breaches register, or the remedial action taken.

Regulatory Requirements

As per the applicable CSP Rulebook and Trustees Code of Conduct, authorised persons are requested to ensure to record all key information in registers which are required to be in place. This information should also extend to any mitigating and/or remedial action undertaken in such circumstances. In this regard, the Authorised Persons are reminded of R3-7.1(vi), R3-7.6, R3-10.1, R3-11.6.2 and R3-11.9.2 of the CSP Rulebook and Sections 6.0 and 9.11 of the Trustees Code of Conduct.

1.6. Filing of Regulatory Submissions

In a few instances, during the supervisory interactions the Authority raised issues relating to late filings of regulatory submissions by authorised persons, such as the Annual Compliance Return and Financial Statements. Such conduct, apart from amounting to breaches of regulatory requirements, may in turn also reflect poor governance practices being adopted in ensuring that the necessary checks and balances are being implemented to ensure compliance with all applicable requirements.

Regulatory Requirements

Authorised persons are expected to have robust systems and controls in place to ensure that regulatory submissions are filed within the stipulated deadlines. Authorised Persons are also expected to have systems to monitor any updates or communications issues by the Authority in this regard. Moreover, the Authority also draws the attention of authorised persons to the Guidance Note on the Methodology to Set Administrative Penalties relating to Non-Material Breaches[5], for further guidance on any penalties which may be imposed by the Authority in cases of non-compliance with applicable deadlines for submission of regulatory submissions.

1.7. Authorised Persons providing Directorship Services

The Authority noted that in two instances where authorised persons offered directorship services, Board meetings were not being held on a regular basis and observed a lack of detail being kept thereon for those held. In one instance, this also resulted in significant delays in the approval of statutory documentation and subsequent late filing with the relevant authorities (e.g. late filing of audited financial statements and annual returns with the Malta Business Registry). The latter, in turn, resulted in the client company incurring penalties for such late submissions.

The Authority also further noted instances where authorised persons were arranging for corporate entities to act as directors/company secretaries for their clients. This is not in line with the CSP Rulebook which sets out that CSPs may only arrange for the appointment of their officers or employees (natural persons) to act as director or secretary, or a similar position, in client entities. In such instances however, the Authority positively noted co-operation by the authorised persons to rectify such deficiencies.

Regulatory Requirements

Authorised Persons providing directorship services are reminded of their general fiduciary duties of loyalty, care and skill, owed to client companies. All directors of companies, and therefore Authorised Persons acting as directors, are expected to act in the best interest of the client company, and to carry out their duties in an honest and transparent way. In this regard, Authorised Persons are expected to

[5] https://www.mfsa.mt/wp-content/uploads/2022/12/MFSA-Guidance-Note-on-the-Methodology-to-Set-Administrative-Penalties-relating-to-Non-Material-Breaches.pdf

ensure that regular client Board meetings are being held and any decisions taken during such meetings duly documented.

Moreover, directors are to ensure that there are no unnecessary delays in the approval and submission of statutory filings, especially for those instances where delays may result in client companies incurring penalties. The Authority had also drawn the attention of all Authorised Persons to these obligations in its Circular issued on 16 September 2020[6].

Authorised Persons are reminded of R3-6.6.3 and R4-3.1–R4-4.4 of the CSP Rulebook. Trustees offering such services should also be guided by the standards of record keeping and reporting in Section Rule 9.6 of the Trustees Code of Conduct relating to Accounting and Record Keeping which requires authorised persons to maintain financial records which permit thorough and satisfactory supervisory activity, as well as be sufficient to comply with any reporting requirements. Therefore, persons providing directorship services are reminded that failures of the nature outlined above are deemed by the Authority to not only be in breach of the Companies Act, but also in breach of the respective legislative and regulatory framework, as applicable.

1.8. Transparency & Cooperation with the Authority

1.8.1. *Notifications of Resignations and Appointments of Approved Persons*

During this Review, the Authority noted a few instances where authorised persons did not inform the Authority, in a timely manner, of resignations of persons holding approved positions. At times, prolonged vacancies in these roles consequently led to a breach of the legal and/or regulatory obligations relating to the minimum board composition or the obligation to appoint a compliance officer. Similarly, the Authority also noted instances where authorised persons failed to seek necessary approvals of the Authority for the appointment of officers prior to submitting the necessary forms to the Malta Business Registry or prior to such persons taking on their respective functions. In such instances, once again the Authority positively noted proactiveness by the authorised persons concerned to implement necessary mitigating measures to avoid the reoccurrence of such events.

Regulatory Requirements

Authorised Persons are requested to ensure that resignations are communicated to the Authority in a timely manner. Resignations should be duly communicated to the Supervision team (fiduciariesoffsite@mfsa.mt) within TCSPs function prior to the effective date of resignation. Furthermore, any proposed appointments should be communicated to the Authorisation Team (autrustscsps@mfsa.mt). It is emphasised that no person may take on a position requiring approval, prior to such approval having been obtained from the Authority.

[6] https://www.mfsa.mt/wp-content/uploads/2020/09/Circular-addressed-to-Companies-and-Individuals-providing-Directorship-Services.pdf

1.8.2. *Provision of Information to the Authority*

Authorised Persons are expected to co-operate with the MFSA, and any other relevant authorities, in an open and honest manner. They are expected to provide the Authority with any information it may require in the exercise of its supervisory role. Whilst the Authority positively noted a general spirit of cooperation when carrying out its work, there was an instance where an authorised person did not demonstrate the expected level of cooperation. This included unjustified delays in the provision of requested documents and/or information, and also, in some instances, resistance to provide information and documents to the Authority.

Regulatory Requirements

Authorised Persons are reminded that they are expected to co-operate with the Authority and any other relevant regulatory authorities in an open and honest manner and shall provide the Authority with any information it may require, in line with R1-2.3 and R3-2.3 of the CSP Rulebook, Section 11.0 of the Trustees Code of Conduct, as well as Sections 1.2.4(ii) and 2.3.2.1.5 of the Corporate Governance Code.

2. Matters relating to the Compliance Function

2.1. Documentation of the Work Carried out by the Compliance Function

The Authority reiterates once again its positive observation related to a notable increase in investment in compliance tools and resources. In the course of its supervisory work, the Authority noted four instances where work carried out by the compliance function was not being documented. Consequently, the Authority was not in a position to assess the matters identified and the checks carried out by the compliance function. In fact, the Authority noted numerous deficiencies in client file reviews and could not determine whether these shortcomings had also been identified and communicated by the compliance function, or whether in fact such deficiencies were being addressed, due to this lack of recording of such work.

On the other hand, the Authority also noted four instances whereby, albeit compliance reports had been drawn up, the recorded compliance work only extended to regulatory updates. In this regard, such reports failed to extend to any compliance checks carried out by the compliance officer, such as: client file reviews, updates on testing/reviews carried out in terms of the Compliance Monitoring Programme, and any weaknesses identified therefrom.

Regulatory Requirements

Authorised persons are to ensure that the work of the compliance function is adequately documented, in line with good governance and record keeping practices. In this regard, the compliance function

should be guided by the compliance monitoring programme, as further set out in the next section. Compliance reports should include any testing/checks carried out, any deficiencies encountered and any corresponding recommendations and/or mitigating measures recommended by the compliance function. Compliance reports should subsequently be duly presented to the Board.

Documentation of compliance work is essential not only for an effective compliance function, but also in terms of good governance, continuity and long-term running of the business. In this regard, reference is made to R2-6.1.3, R3-8.5 and Title 12 of the CSP Rulebook, Article 43(4)(i)(f) of the TTA and Sections 9.4, 9.6 and 9.8 of the Trustees Code of Conduct.

2.2. Compliance Monitoring Programme (the 'CMP')

The CMP is a compliance tool utilised primarily by the compliance function in order to ensure that the Authorised Person is operating in line with applicable legislative and regulatory requirements. The Authority noted two instances where this programme was in fact not in place. In other six instances, this was in place however was not deemed to be adequate, for example due to omission of key compliance checks. Common issues identified included: lack of a set methodology and frequency of testing to be carried and certain missing regulatory checks to ensure compliance with all the applicable legislative and regulatory requirements.

Regulatory Requirements

Authorised persons are requested to have in place and/or strengthen their CMP to ensure that it includes the methodology of the reviews/tests as well as the timeframe by when such tests/reviews are to be carried out. For an effective CMP, the Authority expects the compliance function to conduct a proper risk assessment and mapping exercise to identify and prioritise compliance risk factors prior to the drafting (and updating) of a CMP. The risk assessment should identify areas of high, medium, low compliance risks, identify any gaps in the compliance programme and test the controls in place to mitigate the identified risks. This risk assessment exercise should be data driven (not theoretical), and properly documented and reviewed on a periodic basis.

The CMP should not merely be a tick-box exercise but should be an ongoing programme aimed at monitoring the overall operations and procedures to ensure all aspects of the business are adequately monitored (including all services provided by the Authorised Persons as part of their authorisation) and includes as part of the CMP, such as complaints handling, systems and controls, conflicts of interests, training, breaches, business continuity and its testing, monitoring of critical service providers, capital requirements and professional liability risks, segregation of funds, sampling transactions, AML, Compliance and Due Diligence, record keeping and regulatory calendar submissions.

For each area to be tested, it is recommended that the CMP provides, inter alia:

a) a description of the area to be tested;
b) the relevant procedure explaining how such areas are tested;

c) the finding and/or recommendations; and
d) the period of when the testing will be/was carried out.

The CMP should state the period during which the reviews/tests will take place and once drafted, the program should be presented to the Board for consideration and approval, which should in turn be ensuring effective compliance function monitoring and oversight.

2.3. Carrying out of Compliance Client File Reviews

In two instances compliance-related client file reviews were being carried out sporadically rather than on a pre-set periodical or systematic risk-based basis. In such instances, the Authority noted that the compliance officer of such authorised persons was often reviewing the same clients due to their high-risk rating or only reviewing newly engaged clients. In a few instances, the Authority noted that, albeit certain deficiencies being noted by the Authority relating to missing client documentation kept on file, as required by the authorised person's own internal procedures and checklists, such deficiencies did not feature in the compliance reports prepared by the compliance function. In other instances, compliance reports fell short of including any recommendation to address these gaps.

Regulatory Requirements

Authorised Persons are to ensure that the compliance function is carrying out effective and independent checks on client files, following a set methodology, and ensuring that applicable legislative and regulatory requirements, including internal policies and procedures and those relating to record-keeping, are being adhered to. Furthermore, authorised persons are to ensure that such compliance client file reviews are duly documented, including any weaknesses or breaches identified together with recommendations on the remedial action to be undertaken. Authorised Persons are reminded of R3-8.1 of the CSP Rulebook and Section 9.4 of the Trustees Code of Conduct.

2.4. Independence of the Compliance Officer

The Authority noted instances where Compliance Officers of authorised persons constituted as legal persons were client facing or found to be involved in the Authorised Person's client onboarding process thereby lacking the necessary independence required to fulfil this role. For clarification purposes, compliance officers' involvement in the client onboarding process should only extend to providing guidance with respect to compliance issues, and only if this is deemed necessary.

Regulatory Requirements

Authorised persons are reminded that Compliance Officers should not be involved in the performance of services or activities which they monitor, particularly the process of onboarding of clients, nor should they be client facing. Authorised Persons are reminded of R2-6.1.1 and R3-8.4(i) of the CSP

Rulebook and Section 9.4 of the Code of the Trustees Code of Conduct. On the other hand, and in the spirit of proportionality applied by the MFSA, in relation to CSPs who are natural persons authorised as Under threshold Class A or Under threshold Class B, in terms of, and subject to the conditions set out in R2-6.1.3, such CSPs may fulfil the role of the Compliance Officer themselves.

2.5. Access to all Relevant Information

In one instance, the Authority noted that the compliance officer of an authorised person was not being provided with all relevant and required documentation in order for the said compliance officer to carry out such a role effectively. The Authority highlights that any hindered access to relevant information may result in impeding the compliance officer to carry out the necessary compliance work in an effective manner, resulting in authorised persons adopting a weak Three Lines Model which could in turn result in governance weaknesses.

Regulatory Requirements

Authorised Persons are not only requested to ensure that compliance officers have unhindered access to all relevant documentation, but also that they have adequate resources to carry out their duties. In this regard, Authorised Persons are reminded of R3-8.3 of the CSP Rulebook and Section 2.2.1.2.2.3(i) of the Corporate Governance Code.

3. Matters relating to Record Keeping

3.1. Client Data and Correspondence not Centrally Saved

The Authority noted a few instances where client data and correspondence were not saved centrally. In some cases, records such as client correspondence, were saved in email inboxes of employees, some of whom had left their employment. This led to the inability of authorised persons to provide information to the Authority in a timely manner. Such practices, apart from creating potential obstacles to the Authority's supervisory work, are not reflective of good governance and may also lead to business continuity issues.

Regulatory Requirements

Authorised Persons are requested to ensure that client data and correspondence is centrally saved. The Authority highlights that Authorised Persons are to ensure that records are adequately stored, irrespective of whether these are stored digitally or physically, as long as the method adopted is consistent and conducive to timely retrieval of such records. Authorised Persons are reminded of Title 12 of the CSP Rulebook in particular R3-12.6, Section 9.6 of the Trustees Code of Conduct, as well as

the Circular issued by the Authority on 15 July *2020 titled* ***Circular addressed to all Licence Holders regarding their obligations in relation to record keeping***[7], for further guidance.

3.2. Failure to Segregate Records from Records of Related Entities

In one instance, an authorised person failed to segregate its client records from the records of its related entity. Such practices are not regarded to be in line with adequate governance practices given that they may result in either the authorised person not having all necessary records on file or having client files which include records pertaining to a separate legal entity, which may lead to a risk of breach of confidentiality or legal risk. Furthermore, the Authority also noted a common practice of related authorised persons forming part of a group of entities holding common Board meetings and recording common Board meeting minutes. Specifically, the Authority noted that no indication was made as to which company was servicing the clients discussed in such meetings.

Regulatory Requirements

Authorised Persons are referred to Title 12 of the CSP Rulebook and Section 9.6 of the Trustees Code of Conduct and are reminded of the importance of segregation of records from any other entity, including related entities. In the instance where clients are being serviced by the authorised person and a related entity, separate records must be duly kept. In instances where client data and documentation is shared or relied on, appropriate underlying agreements must be in place governing this arrangement. Furthermore, with respect to common Board meeting minutes being kept, authorised persons are requested to ensure that a clear indication is made as to which related authorised entity is servicing the client/s being discussed in such meetings, and that the Board meeting clearly delineate where specific issues discussed relate a particular authorised entity.

3.2.1. *Non-Recording of Decisions relating to Clients*

The Authority noted a few instances where decisions, or key information, relating to clients or review of client documentation were not being documented. For example, in a number of instances, particularly those where the authorised persons adopted an automated CRA system, the Authority could not find evidence of a system of preparer and reviewer of client documentation, such finding was particularly noted in client risk assessment reviewed. In this regard, authorised persons are reminded to ensure that the preparer/s and reviewer/s of documentation should be duly recorded, as part of the authorised person's internal controls.

Furthermore, in relation to client risk assessments, the Authority also noted instances where key deliberations and information, such as the reason/s leading to a manual lowering of a risk score by the Authorised Person, and/or mitigating measures to be applied to that particular client, were not duly documented. In other instances, it was noted that authorised persons onboarded clients which fell

[7] https://www.mfsa.mt/wp-content/uploads/2020/07/Circular-addressed-to-all-Licence-Holders-regarding-their-obligations-in-relation-to-record-keeping.pdf

outside the Authorised Persons' risk appetite and did not appropriately document the client onboarding decision, nor the implementation of any mitigating measures.

Regulatory Requirements

Authorised persons are referred to Title 12 of the CSP Rulebook and Section 9.6 of the Trustees Code of Conduct for further guidance on record keeping practices which they are expected to implement, as well as the requirements under R3-11.3.1 of the CSP Rulebook, and Sections 3.0 of the Trustees Code of Conduct. Authorised persons are reminded of the importance of the adoption of adequate record keeping practices, and the retention of records which are sufficient to enable the Authority to monitor compliance with the applicable legislative and regulatory regimes.

CONCLUSION

The findings arising from this Review are being highlighted in this letter with the aim of sharing experiences, drawing attention to potential weaknesses in the sector, and to further strengthen governance and compliance culture.

Authorised persons are therefore expected to consider those findings, indicated in this letter, which are applicable to their authorised business. To this end, authorised persons are expected to carry out a gap analysis with respect to the practices and processes of their authorised business and take prompt action to address any identified shortcomings accordingly. This gap analysis should be duly documented and made readily available, to the Authority, upon request. The Authority will be continuously monitoring compliance by TCSPs with the applicable regulatory requirements, as well as the standards and expectations outlined in this Review, through various supervisory interactions, including other Thematic Reviews to be conducted in 2024, to assess the effectiveness of TCSPs' actions following the guidance provided in this Review.

Should anything remain unclear or further guidance on achieving the Authority's expectations in practice be required, authorised persons are invited to contact the Authority, accordingly. The MFSA remains committed to continue providing guidance on best practices to drive enhancements to governance and compliance culture in the financial services sector.

Yours faithfully,

Malta Financial Services Authority

Christopher Peter BUTTIGIEG (Signature)

Digitally signed by Christopher Peter BUTTIGIEG (Signature)
Date: 2024.04.01 13:01:12 +02'00'

Christopher P. Buttigieg
Chief Officer Supervision

Petra CAMILLERI (Signature)

Digitally signed by Petra CAMILLERI (Signature)
Date: 2024.04.01 12:06:37 +02'00'

Petra Camilleri
Deputy Head - Trustees and Company Service Providers Supervision Function