TCM GROUP – DATA PROTECTION MEMORANDUM FOR SENIOR MANAGEMENT

Dear Senior Management.

This document concerns TCM Group International ehf of Suðurlandsbraut 4A, 108 Reykjavík, Iceland, registered at the Icelandic Company Register under No. 650315-0300 **(TCM Group).**

This memorandum summarises the need for a TCM Group-wide program (**Program**) for compliance with privacy and data protection laws (**DP laws**, defined further below) and the obligations imposed on TCM Group's senior management in respect of privacy and data protection compliance in respect of the TCM Alliance and its ethical debt recovery activities as carried out by the TCM Members as set out herein (**Senior Management Compliance**).

The CEO of TCM Group shall oversee compliance with this memorandum, and will liaise with the Group DPO, external lawyers and the Development Manager, as appropriate.

A. DEFINITIONS

DP laws: means any Icelandic or European Union law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument of Iceland or the European Union which implements Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), and the GDPR in each case as amended, consolidated, re-enacted or replaced from time to time, and which applies to a party relating to the use of personal data as well as any other national data protection law which may be applicable to a TCM Member or processing location.

GDPR: means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

TCM Alliance: means the alliance established by TCM Group of independently owned debt collection companies and legal firms acting as individual TCM Members, offering ethical and professional debt recovery solutions to clients on a national and international basis.

TCM Member: means either a "**Shareholder**" (shareholder(s) being members who own 1 (one) Group A and 2 (two) Group C share(s) in TCM Group and have entered into a signed members agreement with TCM Group), an "**Associate Member**" (meaning member(s) of TCM Group who are not Shareholders, and who have entered into a signed associate members' agreement with TCM Group), or an "**Agent**" (meaning member(s) of TCM Group who are not Shareholders, and who have entered into a signed agents' agreement with TCM Group).

TCM Portal: means TCM Group's web-based proprietary portal available at https://platform.tcmgroup.com which is used by TCM Members and TCM Group for the purposes of sending and receiving referrals between the different members of the TCM Group's Alliance to enable efficient national and international debt recovery and further TCM Group's purpose of facilitating cross-border, ethical debt recovery.

B. THE ISSUE

An immense volume of personal data (or personally identifiable information or personal information, as it is sometimes referred to) continues to proliferate and flow daily around the world. Examples concerning TCM Group include personal data flows between TCM Members and via the TCM Portal for the purposes of ethical, cross border debt recovery within the TCM Alliance. Some of this personal data needs to be accessible worldwide, given the location of the TCM Members and individual debtors (who may be based within the European Economic Area (**EEA**) or outside of the EEA.

Information, including personal data, is a valuable asset for TCM Group and the TCM Members. Information assets must be used effectively to meet the TCM Alliance's goals, but regulatory requirements, and individual data subject's and third

parties (such as clients, external advisors, debtors, courts and other third parties) expectations of accuracy and security need to be met. However, DP laws across the world form a complicated patchwork and a failure by the TCM Group to hit the right balance between risk and opportunity in its use of data could have serious consequences for the TCM Alliance in the future.

Personal data is defined broadly and includes and comprises data in relation to any individual who can be identified from that data either directly or indirectly, and personal data processed within the TCM Alliance may include (but is not limited to-:

- Names.
- Contact Information such as addresses and email addresses.
- Dates of birth.
- Social security or other national identification numbers.
- Telephone numbers.
- Financial information of, for example, of debtors where this is relevant to debt recovery matters or revealed by debtors themselves.

TCM Group does not knowingly collect or process personal data from children, except when necessary for and limited to the identification or justification of the debt, and expects the same commitment from all TCM Members, including Senior Management. If Senior Management becomes aware that personal data of children is being processed within the TCM Alliance, it must report it to the CEO immediately.

DP laws have assumed much greater significance in the last few years. In particular, the GDPR, which became law in all EU member states on 25 May 2018 and brought in substantial new compliance requirements and large potential fines (see below). The GDPR applies within the EEA and also to organisations processing personal data to the extent that they are based outside of the EEA if they are processing personal data belonging to EU data subjects or are offering goods and/or services to the EU. This trend is set to continue, particularly with regard to developing laws on security breach in many other countries.

There are many potential ramifications of failing to comply with DP laws, including:

- Adverse publicity, potentially leading to reputational damage and lost trust, for example through data security breaches.
- Missed opportunities and wasted resources.
- Prosecution of or regulatory enforcement action against TCM Group or the TCM Members, resulting in substantial penalties and/or sanctions in different jurisdictions. For example, the GDPR introduces substantial penalties in EEA jurisdictions of up to 4% of annual worldwide turnover of the preceding financial year or EUR 20 million (whichever is the greater).
- Increased scrutiny from regulators whose remits and powers are increasing. For example, the GDPR introduces significantly greater powers of regulators in all EU member states.
- Becoming embroiled in litigation and its attendant time, effort and expense.

These adverse ramifications may affect TCM Group, Senior Management and the individual TCM Members.

The aim of DP laws is generally to ensure good information handling practice, provide accountability of those processing personal data and give rights to individuals. For example, identity theft, stolen personal data and violated privacy policies may result in fraud, theft and deception. Abuse of financial data can have an adverse impact on insurance and credit.

There are various approaches to DP laws worldwide. In many countries, such as all EU member states, privacy is a fundamental right and so has a wide impact on TCM Group's activities. For example, in all EU member states and the EEA, the GDPR specifies that an individual has a fundamental right to have their personal data protected and their personal data may only be processed (that is, obtained, recorded, held, used or disclosed) under certain circumstances.

By contrast, DP laws in the US generally provide protection to individuals interacting in certain sectors only. Various Asia-Pacific countries have taken a different path, in some cases incorporating elements of the two approaches referred to above. For example, there is a European-style privacy commissioner under the regimes in Australia, New Zealand and Hong Kong, while some Asian countries adopt a sectoral approach regarding administration and enforcement.

C. PRIVACY COMMITMENT

A well-constructed and comprehensive TCM Group privacy commitment can provide a solution to these various competing interests and represents an effective risk-management tool. It is essential for privacy compliance and to inform stakeholders such as other TCM Members, debtors, business partners, regulators and the courts of the TCM Group's commitment to compliance with DP laws.

Senior Management's Commitment to ensure compliance with TCM Group's privacy framework

Senior Management of TCM Group has a duty to know about the content and operation of TCM Group's privacy commitment, and to appropriately oversee and ensure its implementation and effectiveness.

Certain DP laws may also specifically require that the Senior Management can demonstrate TCM Group's privacy compliance. For example, the GDPR's accountability principle requires that controllers are able to demonstrate their compliance with the requirements on an ongoing basis.

Elements that TCM Group has implemented and expects Senior Management to oversee and ensure compliance with, include the following:

1. Organizational culture and chain of command

TCM Group must display an organisational culture that encourages compliance and provides all stakeholders, including TCM Members, with the clear guidance they need to achieve it.

TCM Group has implemented a coordinated chain of command (in which the CEO is designated as having ultimate responsibility) which includes seeking and complying with legal advice and IT security advice from external lawyers and IT developers, where applicable.

Senior Management should ensure that they regularly monitor compliance from all stakeholders of TCM Group, obtain feedback from across the TCM Alliance and any other stakeholders, to help TCM Group to take responsibility for the day-to-day compliance of TCM Group with DP laws, regularly reporting back to the CEO.

2. Standards and procedures

- *Privacy Policies*

The privacy policies in place are key elements of TCM Group's compliance obligations.

TCM Members must implement an adequate privacy policy when they are carrying out business within the TCM Alliance. To this end, EEA-based and non-EEA based privacy policies exist depending on the location of the TCM Member.

TCM Group has also implemented a privacy policy covering its own data processing activities.

All Senior Management must ensure that their business has an appropriate privacy policy in force at all times, and must generally monitor during dealings with the TCM Members, that they have implemented their privacy policy correctly (for example, by displaying it on their website or making it available by a link in their email signature).

Amendments are likely to be needed to all privacy policies which must be regularly reviewed. Senior Management must update their own company's privacy policies as required, ensuring that the policy is accessible at every relevant personal data collection point.

- *Lawful Basis*

Generally, TCM Group relies on, and would expect the TCM Members to rely on the following specific grounds for processing which are permitted under the GDPR:

- processing is necessary for the performance of a **contract** to which the individual data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b));
- processing is necessary for compliance with a **legal obligation** to which the controller is subject (the controller being either TCM Group, or the TCM Member, as the case may be) (Article 6(1)(c)); and/or
- processing is necessary for the purposes of the **legitimate interests** pursued by the controller (the controller being either TCM Group, or the TCM Member, as the case may be) or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (Article 6(1)(f)),

save that each TCM Member is free to choose the most relevant lawful basis as they consider fit, in light of their processing activity, the nature of the data concerned and their relationship with the data subject.

When relying on the lawful basis set out at Article 6(1)(f), the following test must be applied by the controller:

- **Purpose test** – is there a legitimate interest behind the processing?
- **Necessity test** – is the processing necessary for that purpose?
- **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?

In the case of debt recovery, processing of an individual's data may have a potentially negative impact on the individual (resulting in a judgment or negatively impacted credit rating). However, this does not automatically mean that the individual's interests outweigh those of TCM Group or the TCM Member. Indeed, processing for debt recovery is considered as a compelling ground for processing by the ICO (the UK supervisory authority and leader in issuing GDPR guidance).

For example, a company (a TCM Member client) may wish to engage a recovery agency (a TCM Member) to carry out debt recovery services. In this case, the company disclose an individual's personal data to the agency (for example, a TCM Member) for this purpose. The company has a legitimate interest in recovering a potential debt it is owed and in order to achieve this purpose it is necessary for them to use the services of a recovery agency to obtain payment.

According to ICO guidance, it is reasonable for individuals to expect that they will have steps taken against them to seek payment of outstanding debts. It is clear that the interests of the individual are likely to differ from those of the company to which they owe money, and also to those of the recovery agency which has an interest in pursuing the debt on behalf of their client(s) and may collaborate with other agencies (via the TCM Alliance) when it requires assistance with debt recovery in a jurisdiction with which it is unfamiliar or does not have appropriate resources. In this situation, the individual may wish to evade paying their outstanding debt.

However, the legitimate interests in passing the personal data to a debt collection agency and the agency processing the personal data on the basis of legitimate interests in these circumstances would not generally be overridden by the interests of the individual. The balance would be in favour of the company and recovery agency, and furthermore, whilst being the subject of debt recovery is undesirable, it is actually in all parties' interests to have the matter resolved, including the individual.

Generally, TCM Group considers that the legitimate interests ground can be satisfied, but this must be verified on a case-by-case basis by each controller. Where appropriate, TCM Group expects all TCM Members to carry out a Legitimate Interests Impact Assessment and supply this to TCM Group or any other TCM Member where possible.

In particular, TCM Group also regularly reviews existing procedures in relation to obtaining individual's **consent** as a legal basis for processing personal data (Article 6(1)(a)), when this is required. TCM Group, and the TCM Members may be required to demonstrate that this consent (where necessary) has been obtained and to ensure that an individual can easily withdraw their consent at any time.

Senior Management should ensure that they regularly monitor compliance from all stakeholders of TCM Group, obtain feedback from across the TCM Alliance and any other stakeholders, to help TCM Group to take responsibility for compliance, by reporting any issue related to **consent** or **any other lawful basis (especially in respect of any basis based on the use of legitimate interests)** back to the CEO, where this is likely to bring risk or exposure to TCM Group.

- *Data Subject Requests*

TCM Group must also be in a position at all times to respond promptly to an individual's request relating to their personal data held by TCM Group or processed on the TCM Portal (such as for a copy of all of the personal data held or to erase all such personal data). Furthermore, all TCM Members must be able to comply with such requests pursuant to the DP laws.

Senior Management should ensure that they regularly monitor compliance from all stakeholders of TCM Group, obtain feedback from across the TCM Alliance and any other stakeholders, to help TCM Group to take responsibility for compliance, by reporting any issue related a data subject request, or any data subject request that has been made in relation to personal data processed pursuant to the TCM Alliance, back to the CEO, where this is likely to bring risk or exposure to TCM Group.

- *Confidentiality, Security and Data Breaches*

TCM Group takes information security seriously and has undertaken an audit of the TCM Portal to protect the security, confidentiality and integrity of personal data held within the TCM Portal, which includes seeking and complying with IT security advice from external IT developers.

Certain DP laws may also require that TCM Group (or the relevant controller) notify relevant regulator(s) of data breaches. For example, the GDPR requires that businesses notify the relevant regulator of all data breaches without undue delay and where feasible within 72 hours.

TCM Group therefore requires all TCM Members to implement appropriate security and confidentiality measures, as well as plans for any security breach and data restoration plan in the event of any loss, damage, destruction or unauthorized access to data processed within the TCM Alliance. TCM Group expects Senior Management to lead the example by implementing these measures.

Senior Management should ensure that they regularly monitor compliance from all stakeholders of TCM Group, obtain feedback from across the TCM Alliance and any other stakeholders, to help TCM Group to take responsibility for compliance, by reporting any security, loss, destruction or unauthorized access issues related personal data processed pursuant to the TCM Alliance, including any suspected or actual data breach, back to the CEO, as soon as possible.

- *Contracts*

TCM Group has developed appropriate contractual strategies as a risk management tool.

This has included ensuring relevant appropriate contractual documentation has been implemented where required, such as a Data Transfer Agreement between TCM Members and TCM Group, a Portal Agreement for use of the TCM Portal by TCM Members as well as a Data Processing Agreement between the TCM Members and TCM Group (**TCM Documentation**). Such agreements will be reviewed periodically to ensure compliance, and will be issued to all new TCM Members before such new TCM Members are able to undertake any data processing activities.

TCM Group leads by example, and therefore expects that the Senior Management conclude such TCM Documentation where required. Senior Management should ensure that they regularly monitor compliance from all stakeholders of TCM Group, obtain feedback from across the TCM Alliance and any other stakeholders, to help TCM Group to take responsibility for compliance, by reporting contractual breaches or non-compliance with the TCM Documentation by any TCM Member, back to the CEO.

- *Cross border transfers*

TCM Group has reviewed its procedures for cross-border data flows including how it transfers personal data from one

jurisdiction to another, particularly when transfers occur from the EEA to a country based outside of the EEA.

To this end, TCM Group has also prepared appropriate Commission Standard Contractual Clauses for transfers from countries within the EEA to countries outside of the EEA which have been signed up to by all TCM Members and will be issued to new members as they join the TCM Alliance. No TCM Member will be entitled to process or transfer personal data internationally within the scope of the TCM Alliance without having first adhered to these clauses.

Furthermore, TCM Group considers that the TCM Alliance can also, as a back-up position, rely on Article 49(1)(e) of the GDPR, which states that transfers of personal data from the EEA to a non-EEA territory may take place when: *"the transfer is necessary for the establishment, exercise or defense of legal claims"*.

Recital 111 of the GDPR states that a transfer can be made where it is: *"occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies"*.

The ICO also provides for a wide definition of what a legal claim is, stating that:

"The claim must have a basis in law, and a formal legally defined process, but it is not just judicial or administrative procedures. This means that you can interpret what is a legal claim quite widely, to cover, for example, all judicial legal claims, in civil law (including contract law) and criminal law. The court procedure does not need to have been started, and it covers out-of-court procedures. It covers formal pre-trial discovery procedures."

This can be applicable to cross-border debt recovery claims carried out by the TCM Alliance and for international data transfers carried out by TCM Members, including via the TCM Portal.

TCM Group is therefore satisfied that it has used all reasonable efforts to ensure relevant safeguards in place regarding international transfers between TCM Members, including via the TCM Portal for TCM Alliance business. Nonetheless, it is the responsibility of each TCM Member to ensure such transfers are conducted lawfully and that any TCM Member based outside of the EEA is lawfully received, processed and stored, pursuant to any applicable law in the receiving jurisdiction.

Again, TCM Group leads by example, and therefore expects that the Senior Management do so as well. Senior Management should ensure that they regularly monitor compliance from all stakeholders of TCM Group, obtain feedback from across the TCM Alliance and any other stakeholders, to help TCM Group to take responsibility for compliance, by reporting any issues it encounters regarding international transfers, back to the CEO.

- *Ongoing commitment*

TCM Group has an ongoing commitment to privacy matters and regularly considers how it develops new products, services or other activities which affect personal data. For example, the GDPR requires businesses to implement "privacy by design" (for example, when creating new products, services or other activities that process personal data) and "privacy by default" (for example, data minimisation). TCM Group also carries out "data protection impact assessments" where required to do so, (and taking into account the nature, scope, context and purposes of the processing.

3. Training and enforcement

Effective compliance training programs may be implemented from time to time for Senior Management and TCM Members.

Failings to adhere to the DP laws by TCM Group, TCM Members and/or the Senior Management are taken very seriously. TCM Group will take appropriate action in respect of sufficiently serious failings which bring TCM Group into disrepute or expose TCM Group and the TCM Alliance or other TCM Members to risk.

4. Regular reviews

From time to time, TCM Group will review and update its data protection and privacy commitments in the light of new laws, developments and business activities and any regulatory or legal changes to the legal-basis for cross-border data flows.

TCM Group requires that Senior Management keep themselves generally updated with any new DP laws or guidance and ensure that they are aware of the latest and up to date TCM Group privacy commitment.

D. SENIOR MANAGEMENT COMPLIANCE

The above represents only a short synopsis of the requirements of DP laws, with particular examples given of only some of the requirements introduced by the GDPR across the EU and those on which TCM Group places the most importance. There are many more requirements that are not included in this note for the sake of brevity. Continuing to comply with all of the compliance requirements of all of the relevant DP laws that will impact TCM Group's activities needs ongoing commitment from all stakeholders.

The adherence to these principles and the DP law by Senior Management, in respect of the TCM Alliance and when conducting their own business activities, forms part of the Senior Management Compliance, which TCM Group requires from all Senior Management.

Once you have read and understood this Data Protection Memorandum and the Senior Management Compliance required of you, please confirm that you have done so by signing and returning the attached copy to the CEO.

If you have any questions about this document, please contact the CEO using the following details: email: ceo@tcmgroup.com : phone +44 (0) 79 799 13496.

I, SHAUN DUNCAN (name), acknowledge that on 21 NOVEMBER 2019 (date), I received a copy of the TCM Group Data Protection Memorandum for Senior Management and conform that I have read and understood it and agree to abide by its terms.

Signature .....