Pursuant to the notice provided on 25 September 2023, We Track Software Ltd has added the following subcontractors:

Forta, LLC d/b/a Alert Logic – United States of America	MDR solutions provide single pane-of-glass visibility across public cloud, hybrid, and on-premises environments, providing vital insights on your security posture, and detecting and responding to threats to your business.
Productboard, Inc. - United States of America	Used to capture user feedback and new ideas for the product teams
Pendo.io, Inc. United States of America	Used to capture usage information of our product offerings
Caffeinated Corporation/US	Used by Customer Support to streamline and automate support processes.
Smartlook.com, s.r.o., Czech Republic	User experience and customer journey monitoring within WeTrack to gain insights and improve functionality; Customer name and email can be made available, can be anonymised.

Data Processing Addendum (DPA)

This Data Processing Addendum (DPA) is by and between the responsible party Customer listed on the Order Form (hereinafter referred to as "**Customer**") and the contract processor, We Track Software Ltd. (herein referred to as "**Provider**").

Preamble
This DPA sets out in concrete terms the data protection obligations of the contracting parties, which arise from the contractual relationship between the parties and is hereby incorporated into any existing and currently Order Form/Offer/Service Agreement including Provider's Master Subscription Terms and Conditions, Maintenance Agreement, and/or Cloud Hosting Agreement; hereinafter collectively referred to as "Service Agreement". This DPA shall apply to all activities wherein employees of the Provider or persons commissioned by the Provider process Personal Data of the Customer. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Service Agreement.

Data Ownership

1. The Provider acknowledges and agrees that as between the parties, the Customer Personal Data and all Intellectual Property Rights in the Customer Personal Data shall belong to the Customer to the fullest extent possible. The Provider hereby assigns and shall procure that its agents and subcontractors shall assign (by way of present and future assignment) to the Customer absolutely all its rights, title and interest (if any) in respect of the Customer Personal Data and the Intellectual Property Rights in and to the Customer Personal Data with the intent that such property and Intellectual Property Rights shall, if they are in existence, forthwith vest in the Customer and shall, if they are yet to come into existence, vest in the Customer forthwith upon the same coming into existence.

2. The Customer hereby grants the Provider a royalty-free licence during the Term to use, edit, create databases from, copy and store the Customer Personal Data solely for the purposes of performing and fulfilling its obligations under this DPA (but for no other purpose).

3. The Customer warrants that it has the legal right to disclose all Customer Personal Data that it does in fact disclose to the Provider under or in connection with the DPA.

Data Processor Obligations

4. The Provider acts as a Data Processor in respect of the Customer Personal Data it Processes on behalf of the Customer in accordance with the terms of this DPA.

5. The Customer is a Data Controller in respect of the Customer Personal Data and shall comply with its obligations as a Data Controller under Data Protection Law.

6. The Provider shall comply with its obligations as a Data Processor under Data Protection Law, which shall include compliance with the Data Security Obligations. If the Provider is or becomes aware of any reason that would prevent its compliance with Data Protection Law or any incident of non-compliance with Data Protection Law in connection with the Processing of Customer Personal Data under this DPA it shall notify the Customer in the most expedient time possible.

7. The Provider agrees that it will only Process the Customer Personal Data in accordance with this DPA and any other written instructions of the Customer.

8. Each of the Parties acknowledges and agrees that Appendix 1 to this DPA is an accurate description of the Processing of Personal Data carried out by the Provider. Appendix 1 sets out the scope, nature and purpose of the Processing of the Customer Personal Data by the Provider, including the type of Customer Personal Data Processed, the relevant categories of Data Subjects, and an up to date list of relevant subcontractors who may require to Process Customer Personal Data as part of the fulfilment of all the Provider's obligations under this DPA.

Provider's Personnel

9. The Provider will ensure that its key personnel who Process Customer Personal Data under this DPA

    a. are subject to appropriate obligations of confidentiality;
    b. have undergone reasonable levels of training in Data Protection Law; and,

c. are aware of both the Provider's duties and their personal duties and obligations under Data Protection Law and this DPA.

Data Collection

10. The Provider will only collect Customer Personal Data for the Customer using a lawful basis as set out in the Provider's data privacy policy (to be maintained and updated periodically). Such privacy policy shall inform the User or Data Subject as the case may be of the Provider's identity, the purpose or purposes for which their Personal Data will be processed, and any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair processing.

Data Subject Requests and Regulators

11. The Provider agrees to assist the Customer within such reasonable timescale as may be specified by the Customer with all Data Subject rights requests received from the Data Subjects of the Customer Personal Data Processed in connection with this DPA. Should the Provider receive any such requests directly, the Provider will immediately inform the Customer that it has received the request and forthwith forward the request to the Customer. The Provider will not respond in any way to such a request, except on the instructions of the Customer.

12. The Provider agrees to assist the Customer within such reasonable timescale as may be specified by the Customer with the conduct of Data Protection Impact Assessments and Prior Consultation requests in connection with the Processing of Customer Personal Data under this DPA.

13. The Provider will maintain complete and accurate records such as a data processing map, and a data breach response procedure, to demonstrate compliance with Data Protection Law and best practice.

14. The Customer agrees that the Provider may charge a moderate administration fee (on a time spent basis using hourly rates) for any recorded instances of assistance provided to the Customer or a Data Subject in connection with clauses 11 – 13 and clause 25 above a de minimis level (of 1 hour per month) ("Data Support Fees"), where any assistance at or below the de minimis level in any month shall not be chargeable.

Cross Border Transfers of Customer Personal Data

15. The Provider will not transfer any Customer Personal Data outside of the UK or the European Economic Area which does not comply with either the GDPR or UK GDPR rules on restricted transfers of personal data to third countries. If such a transfer is due to be made, the Provider shall ensure that a suitable transfer mechanism (one that provides appropriate safeguards in the terms set out in Articles 44 to 50 of the GDPR) is selected, and as a default the Provider shall select and apply the standard contractual clauses as approved by the European Commission or Information Commissioner's Office (as appropriate) unless another suitable transfer mechanism is agreed between the Provider and the relevant entity .

16. In the event that the chosen transfer mechanism entered into under Clause 015 ceases to be valid, the Provider shall
    a. enter into and/or procure that any relevant third-party / subcontractor enters into another permissible data transfer mechanism;
    b. destroy any Customer Personal Data in its and/or its subcontractor's possession; or
    c. return any Customer Personal Data in its and/or its subcontractor's possession to the Customer.

Subcontractors

17. The Provider may only engage a new third-party (subcontractor) to process the Customer Personal Data if:
    a. the Customer is provided with an opportunity to object to the appointment of each subcontractor within three working days after the Provider supplies the Customer with full details in writing regarding such subcontractor;
    b. the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures;
    c. the Provider maintains overall control of the Customer Personal Data it entrusts to the subcontractor; and the subcontractor's access to Customer Personal Data will terminate on termination of this DPA for any reason.

18. Those subcontractors approved as at the commencement of this DPA are as set out in Appendix 1 to this DPA.

19. Where the subcontractor fails to fulfil its obligations under the written agreement with the Provider which contains terms substantially the same as those set out in this DPA, the Provider remains fully liable to the Customer for the subcontractor's performance of its DPA obligations.

20. The Parties agree that the Provider will be deemed by them to control legally any Customer Personal Data controlled practically by or in the possession of its subcontractors.

21. On the Customer's written request, the Provider will endeavour to audit a subcontractor's compliance with its obligations regarding the Customer Personal Data and provide the Customer with the audit results (subject to all applicable laws). Where the Customer and Provider conclude that the subcontractor is in material default of its obligations regarding the Customer Personal Data, the Provider shall contact the subcontractor to remedy such deficiencies within 21 days.

Data Security

22. The Provider must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Customer Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Customer Personal Data.

23. The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

    a. the pseudonymisation and encryption of personal data;
    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of We Track Software's processing systems and services;
    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
    d. a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

Data Breaches

24. The Provider will notify the Customer within 24 hours of becoming aware of a Data Security Breach and shall follow-up with a detailed description in writing, including the cause of the breach, remedial action taken and the potential consequences of the breach) and support the Customer in any notification of the breach to Regulators and/or Data Subjects.

25. Immediately following any Data Security Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Provider will reasonably co-operate with the Customer including but not limited to:

    i. assisting with any investigation;
    ii. providing the Customer with physical access to any facilities and operations affected;
    iii. facilitating interviews with the Provider's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;
    iv. making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Law or as otherwise reasonably required by the Customer; and
    v. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Data Security Breach.

26. The Provider will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Data Security Breach without first obtaining the Customer's consent, except when required to do so by domestic or EU law.

Indemnity

27. The Provider shall indemnify the Customer and keep the Customer indemnified up to the limits defined in clause 12.8 of the DPA against all losses, damages, penalties, fines, costs, expenses or other liabilities (including reasonably and necessary legal fees) incurred by, awarded against or agreed to be paid by the Customer arising out of or in connection with:

    a. any breach by the Provider, the Provider's personnel and/or the Provider's sub-contractors of this DPA or any Data Protection Law; and

b. any act or omission of the Provider, the Provider's personnel and/or the Provider's sub-contractors which puts the Customer in breach of its obligations under Data Protection Law.

Appendix 1: Data processing purposes and details

Details of the Processing of Customer Personal Data by the Provider as required by the GDPR and UK GDPR.

Types of Personal Data	Name, email address and telephone numbers of Users.
Categories of Data Subject	Individuals that are Users (individual employees, advisors, agents, officers and sub-contractors of the Customer).
Subject matter and duration of the Processing of Customer Personal Data	This is set out in the Proposal under Permitted Purpose and the We Track Standard Terms and Conditions of business
The nature and purpose of the Processing of Customer Personal Data	To set up Users with log ins, allow system notifications, to deal with support queries, permit communication flows, maintain a record of Users, and to manage the account.
The obligations and rights of the Customer	These are set out in the Proposal and T&Cs.

Approved Subcontractors:

Sub-processor / Country	**Services**
Momentus Affiliates: - **Ungerboeck Systems International, LLC; United States of America and New Zealand** - **Ungerboeck Software International, Pty Ltd.; Australia and New Zealand** - **Oletha Pyt Ltd; India** - **Ungerboeck Systems International GmbH; United Kingdom**	Support for the contract execution: • Support services ("Follow-the-Sun") and technical services; • Alpha/Beta/Early Adopter Program; • Web sessions and online meetings; • Remote or on-site services; • Technical monitoring of the cloud environment (availability and performance monitoring, as well as troubleshooting in the event of a malfunction or outage outside of Customer's regular office hours); • Applies to non-hosted (on-premises) customers only: For support tests it may be necessary to test with the Customer's actual data, to be able to reproduce an error. For this purpose, the Customer is asked to provide a copy of his database via MediaShuttle (alternatively, the Customer can upload the database copy to the secured EU FTP server).
Zendesk, Inc., United States of America	Support center and knowledge base Ticket system for processing support tickets for Momentus software, provision of the platform, servers are located in the USA.
Delighted, LLC, United States of America	Collection of customer feedback – integrates with Zendesk; customer name and email is collected and visible.

Atlassian, Australia	Dev, IT, Security, Finance, HR helpdesk; integrates with Zendesk and customer information can be pushed to this system
Intercom R&D Unlimited Company, Ireland	Live chat, support center and knowledge base Ticket system for processing support tickets for WeTrack software.
Smartlook.com, s.r.o., Czech Republic	User experience and customer journey monitoring within WeTrack to gain insights and improve functionality; Customer name and email can be made available, can be anonymised.
Altaa Vistaa Business Solutions Pvt Ltd, India	Customer Success Services, other contractual services (mainly assigned for, but not limited to, English speaking projects)
Stripe, Inc., United States of America	Upon subscription of the proposed services (Momentus Payments / Payment Processing Services through Momentus Software)
DocuSign Inc., United States of America	Upon subscription of the proposed services (Electronic Signature integration in Momentus Software including – if applicable - envelope provision)
Jotform, Inc., United States of America	Upon subscription of the proposed services (Implementation of online forms)
Dynatrace, LLC, United States of America	Third party monitoring and logging platform that Momentus uses for ingesting, parsing, querying, and performing analytics on Momentus applications and infrastructure logs.
Microsoft Azure - EU	Hosting Provider
Twilio (owners of SendGrid) United States of America	Email delivery, API and marketing service

Data Protection Officer:

Ken Bell - Ken.bell@gomomentus.com

Legal Contact/General Counsel

Matthew Epps- Matt.Epps@gomomentus.com