EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3701 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with [choose relevant option: OPTION 1: Article 28(3) and (4) of Regulation (EU) 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] / [OPTION 2: Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data].

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons

authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/ shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 /

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s):

Processor:

Raterware

Vejsgårdtoften 10,

4241, Vemmelev, Denmark

Contact person:
Martin Vestenkjær CEO

support@raterware.com

+45 6142 0268

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed:

Employees and Team Members: *These are the individuals whose performance and related data (ratings, evaluations, etc.) are processed within the Raterware platform. This includes employees or team members being evaluated by managers or supervisors.*

Managers and Supervisors: *These are users responsible for inputting data related to team evaluations, managing teams, and assessing employee performance. Their personal data may include login credentials, contact details, and activity related to managing the platform.*

HR Personnel and Administrators: *This includes users who oversee the implementation of the platform, access reports, or manage administrative tasks. Their personal data may be used for account management and ensuring compliance with internal processes.*

Clients or Companies Using Raterware: *If the platform is used by external companies or clients to manage their teams, their data could also be processed, including contact details and payment information for subscription purposes.*

Data Controller vs Data Processor

In the context of the General Data Protection Regulation (GDPR), Raterware acts as a ***Data Processor****, while our customers (businesses, managers, and organizations using Raterware) act as the* ***Data Controllers****.*

- *The* ***Data Controller*** *is responsible for determining the purposes and means of processing personal data. This typically includes businesses or organizations that use Raterware's platform to evaluate and manage their employees or team members.*
- *Raterware, as the* ***Data Processor****, processes personal data on behalf of the Data Controller in accordance with their instructions and the terms outlined in our agreement. Raterware does not determine the purpose or legal basis for processing personal data—that responsibility lies with the Data Controller.*

Raterware processes personal data to fulfill the following purposes on behalf of the Data Controller:

- *Employee/team member evaluations and performance tracking.*
- *Generating analytical reports and insights based on the data provided by the Data Controller.*
- *Managing team structures and sending automated notifications regarding evaluation deadlines.*

Categories of personal data processed:

Identification Data:

- *Name*
- *Email address*
- *User ID or unique identifiers*
- *Company or organization name*

Performance Data:

- *Evaluation and rating scores*
- *Historical performance trends and reports*
- *AI-generated insights based on performance metrics*

Login and Account Data:

- *Username and password (encrypted)*
- *Authentication and authorization logs*
- *Session activity and login history*

Usage Data:

- *Interaction with platform features (e.g., number of evaluations, dashboard interactions)*
- *Activity logs (e.g., data submission, report generation)*
- *User preferences and settings*

Subscription and Payment Information (where applicable):

- *Payment details (processed via third-party, e.g., Stripe)*
- *Subscription tier or plan*
- *Billing information (company name, address, etc.)*

Technical Data:

- *IP address*
- *Browser type and version*
- *Device information (e.g., mobile vs. desktop)*
- *Cookies and session tracking data*

Sensitive data processed and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

To ensure the safety and confidentiality of any potentially sensitive data, Raterware has implemented the following safeguards:

1. ***Purpose Limitation:***
    - *Sensitive data, if processed, is collected solely for the purpose of performance management and employee development. It is not used for any unrelated purposes.*
2. ***Access Restrictions:***
    - *Access to any sensitive data is restricted to authorized personnel only, such as managers or supervisors, based on their defined roles within the organization.*
3. ***Data Encryption:***
    - *All sensitive data is encrypted in transit and at rest using industry-standard SSL/TLS encryption and database encryption protocols to ensure unauthorized access is prevented.*
4. ***Audit and Monitoring:***
    - *All access to sensitive data is logged, and regular audits are performed to track who accessed the data and when.*
5. ***Onward Transfers:***
    - *Sensitive data is not transferred to third parties unless strictly necessary for the performance of Raterware's services, and only after obtaining explicit consent from the user. Any transfers to sub-processors are governed by Data Processing Agreements (DPAs) ensuring full compliance with GDPR.*
6. ***Data Minimization:***
    - *Only the minimal amount of sensitive data necessary to fulfill the purpose of the service is collected and processed. Raterware follows strict data minimization principles.*
7. ***Additional Security Measures:***
    - *Multi-factor authentication (MFA) is used to secure access to systems that handle sensitive data.*
    - *Regular security audits and penetration testing are conducted to identify and address potential vulnerabilities.*

Nature of the processing:

Raterware processes personal data for the purpose of providing performance management, team evaluation, and employee development services. The nature of the processing involves:

2. ***Collection:***
    - *Raterware collects personal data provided by users (managers, team leaders) during the setup of accounts and the use of the platform, including performance evaluations and feedback.*
3. ***Storage:***
    - *Personal data is securely stored in Raterware's cloud-based infrastructure (Heroku) to facilitate ongoing access and analysis. All data is encrypted during storage to ensure confidentiality.*
4. ***Analysis:***
    - *Raterware processes personal data to generate AI insights and recommendations to managers, including performance trends, team dynamics, and individual strengths and weaknesses. This analysis is used to enhance employee development, assess team performance, and identify areas for improvement.*
5. ***Consultation:***
    - *Authorized users, such as managers and team leaders, can access the platform to view and consult reports, insights, and evaluations based on the collected and processed data.*
6. ***Transfer (if applicable):***
    - *In cases where sub-processors are involved (e.g., for hosting or analytics services), personal data may be securely transferred under the safeguards provided by Data Processing Agreements (DPAs) and Standard Contractual Clauses (SCCs). These transfers are done exclusively for purposes related to the performance of Raterware services.*
7. ***Deletion or Anonymization:***
    - *Upon user request or upon termination of service, personal data is either securely deleted or anonymized, ensuring that no personally identifiable information remains accessible. Raterware follows data retention policies that comply with GDPR guidelines.*

Purpose(s) for which the personal data is processed on behalf of the controller:

1. ***Employee Performance Evaluation and Management:***
    - *To facilitate the evaluation of individual and team performance by providing a structured and objective system for rating employees based on specific metrics. This enables the controller to track progress, assess competencies, and make data-driven decisions regarding performance improvement.*
2. ***Data-Driven Insights and Reporting:***
    - *To generate AI-driven insights and reports that analyze employee performance trends, identify strengths and areas for improvement, and support strategic decisions related to talent management, development, and succession planning.*
3. ***Team and Organizational Development:***
    - *To support the controller in building stronger teams by providing analysis on team dynamics, individual contributions, and overall performance trends, helping to create development plans and improve collaboration within teams.*
4. ***Compliance and Record-Keeping:***
    - *To ensure compliance with organizational policies, labor laws, and performance-related legal requirements by maintaining accurate and up-to-date records of performance evaluations and employee feedback.*
5. ***Training and Development Recommendations:***
    - *To assist in identifying skill gaps and recommending targeted training and development opportunities based on individual performance data, helping the controller enhance employee skills and performance over time.*

Duration of the processing:

Raterware processes personal data for the duration of the contractual relationship between the controller (the organization using Raterware) and Raterware. Personal data will be retained as long as the controller continues to use Raterware's services, unless otherwise directed by the controller or required by law.

- ***Upon Termination of the Contract:***
    - *Upon termination of the contract or at the request of the controller, all personal data will be deleted or returned within a maximum period of 30 days, in accordance with the controller's instructions, unless further retention is required by applicable law.*

This ensures that data processing will be carried out only as long as necessary to fulfill the services provided by Raterware and complies with data retention policies and GDPR requirements.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing:

Processing by (Sub-)Processors

Subject Matter of Processing: Raterware engages with sub-processors to facilitate the delivery of its platform services. The processing includes hosting, storage, authentication, payment processing, communication, and email distribution, as well as other technical infrastructure and support services necessary for the smooth operation of Raterware's services. Sub-processors are involved to ensure high availability, secure data handling, and effective service delivery.

Nature of Processing:

Data Hosting & Storage: Sub-processors such as Heroku provide cloud infrastructure and database services to securely store, back up, and manage user data within the platform.

Authentication & Security: Sub-processors like Auth0 handle user authentication and identity management services, ensuring secure access control.

Payment Processing: Stripe processes financial information for payment transactions and subscription management, ensuring compliance with financial security standards (e.g., PCI-DSS).

Email Distribution & Communication:

Mailchimp is used for automated email notifications, such as team evaluation reminders or platform updates.

Technical Support Services: Some sub-processors may provide support for troubleshooting or system maintenance.

Duration of Processing:

Sub-processors process personal data for as long as required to deliver their services during the term of the contractual relationship between Raterware and the controller. Upon termination of the contract or upon request of the controller, the data processed by sub-processors will be returned or deleted in compliance with applicable laws and contractual agreements. Each sub-processor follows the same retention and deletion policies as described in Raterware's core agreements.

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures need to be described concretely and not in a generic manner.

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

1. ***Measures of Pseudonymisation and Encryption of Personal Data:***
    - *All personal data transmitted between clients and the Raterware platform is encrypted using SSL/TLS protocols (HTTPS), ensuring secure transmission.*
    - *Sensitive data, such as personally identifiable information (PII), is encrypted at rest using advanced AES-256 encryption methods within our databases hosted on Heroku.*
    - *Pseudonymisation techniques are applied to minimize the identification of individual data subjects wherever feasible, especially during data analysis and reporting stages.*

2. ***Measures for Ensuring Ongoing Confidentiality, Integrity, Availability, and Resilience of Processing Systems and Services:***
    - *Role-based access control (RBAC) is enforced to ensure that only authorized personnel have access to personal data. Each user is granted the least amount of privilege necessary for their tasks.*
    - *Our platform is hosted on highly resilient infrastructure (Heroku and AWS), which includes failover systems and automated backups to ensure continuous service availability.*
    - *Data integrity checks are embedded into system operations to detect any unauthorized changes or corruptions of data.*

3. ***Measures for Ensuring the Ability to Restore Availability and Access to Personal Data in a Timely Manner in the Event of a Physical or Technical Incident:***
    - *Automatic daily backups of databases are stored securely and can be restored within a defined recovery time objective (RTO) of less than 24 hours in the event of a data breach or loss.*

4. ***Measures for User Identification and Authorisation:***
    - *Multi-factor authentication (MFA) is mandatory for all administrative accounts with access to sensitive data or systems, enforced through our identity management provider (Auth0).*
    - *OAuth 2.0 protocols are used for authentication of external systems and users, ensuring secure access token generation and management.*

5. ***Measures for the Protection of Data During Transmission:***
    - *Data in transit is protected using TLS 1.2/1.3 with strong cipher suites to prevent eavesdropping or tampering.*
    - *Secure APIs and WebSockets ensure encrypted communication between clients, servers, and third-party sub-processors.*

6. ***Measures for the Protection of Data During Storage:***
    - *All stored personal data is encrypted at rest using AES-256 encryption standards.*

7. ***Measures for Ensuring Physical Security of Locations Where Personal Data is Processed:***
    - *Raterware's data is hosted on Heroku's cloud platform, with all data centers certified under ISO 27001, SOC 1, SOC 2, and SOC 3 standards, ensuring stringent physical security controls.*

8. ***Measures for Ensuring Events Logging:***
    - Detailed logging of all system events, including access logs, data modifications, and system changes, is maintained.
    - Raterware uses Papertrail for centralized logging and monitoring of system events in real-time. Logs include server errors, access control failures, performance bottlenecks, and operational activities that could impact the security and availability of personal data.
    - Logs are transmitted securely to Papertrail using TLS encryption to ensure that no unauthorized parties can intercept or modify logs during transit.
    - Role-based access control (RBAC) is applied to logs in Papertrail to ensure that only authorized personnel can access logs, and logs are searchable for the purpose of troubleshooting and compliance audits.
    - Logs are retained for a period in accordance with Raterware's data retention policies and are securely deleted after the retention period.
    - Logs are regularly monitored for suspicious activities, and alerts are configured for any critical security or operational events.
    -

9. ***Measures for Certification/Assurance of Processes and Products:***

   - *Raterware's data protection processes are continuously evaluated, with certifications such as ISO 27001 and SOC 2 compliance from key partners (Heroku).*

10. ***Measures for Ensuring Data Minimisation:***

    - *We only collect the minimum amount of personal data necessary for the services we provide.*
    - *Data retention policies ensure that personal data is kept only for as long as necessary to fulfill its intended purpose.*

11. ***Measures for Allowing Data Portability and Ensuring Erasure:***

    - *Data subjects can request to export their personal data in a machine-readable format at any time through our platform.*
    - *Upon request, personal data can be permanently erased from our systems following GDPR-compliant processes.*

12. For transfers to (sub-) processors:

- *All sub-processors are required to maintain an equivalent or higher level of security, and compliance with GDPR is ensured through DPAs and regular security assessments.*

ANNEX IV: LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

The controller has authorised the use of the following sub-processors:

Sub processors

Sub-processor	Service	GDPR state
Heroku (Salesforce)	Infrastructure Hosting	Complies with GDPR. Heroku is part of Salesforce, which has EU data protection measures in place.
Auth0	User Authentication	GDPR compliant. Auth0 provides data processing agreements and follows EU data protection guidelines.
Stripe	Payment Processing	Fully GDPR compliant. Stripe has strong data protection measures and offers a GDPR-compliant Data Processing Agreeme
Mailchimp (The Rocket Science Group)	Email Communication & Marketing	GDPR compliant. Mailchimp offers a GDPR-compliant DPA and follows EU privacy regulations.
GitHub	Code Repository Hosting	GDPR compliant. GitHub, a Microsoft subsidiary, follows the GDPR and offers a DPA for customers.
Papertrail (SolarWinds)	Log Management	GDPR compliant. Papertrail follows GDPR guidelines, offering secure log storage and encryption.

1. **. Name: Heroku (Salesforce)**
    - **Address:** The Landmark @ One Market St., Suite 300, San Francisco, CA 94105, United States
    - **Contact person's name, position, and contact details:**
      Name: Contact Heroku Support
      Email: support@heroku.com
      Phone: +1 (866) 278-6750
    - **Description of the processing:**
      Heroku provides the infrastructure for hosting Raterware's platform. It is responsible for storing, processing, and securing data within the EU. They ensure high availability, encrypted storage, and continuous monitoring of all databases. Heroku is accountable for physical and network-level security. Raterware handles application-level security and data processing logic.

---

2. **2. Name: Auth0**
    - **Address:** 10800 NE 8th St, Suite 700, Bellevue, WA 98004, United States
    - **Contact person's name, position, and contact details:**
      Name: Auth0 Support
      mail: support@auth0.com
      Phone: +1 (888) 235-2699
    - **Description of the processing:**
      Auth0 manages user authentication for Raterware, including login credentials and access control. They are responsible for handling secure token-based authentication (OAuth) and ensuring user identity verification across Raterware's services. Raterware configures which data points are exchanged during the authentication flow.

---

3. **3. Name: Stripe**
    - **Address:** 510 Townsend St, San Francisco, CA 94103, United States
    - **Contact person's name, position, and contact details:**
      Name: Stripe Support
      Email: support@stripe.com
      Phone: +1 (877) 787-7473
    - **Description of the processing:**
      Stripe handles payment processing for Raterware's subscription services. Stripe processes customer payment information, handles billing and subscription renewals, and manages secure transactions. Stripe is responsible for PCI compliance, payment security, and managing sensitive payment data, while Raterware maintains the customer relationship and manages subscription tiers.

---

4. **4. Name: Mailchimp (The Rocket Science Group)**
    - **Address:** 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308, United States
    - **Contact person's name, position, and contact details:**
      Name: Mailchimp Support

Email: support@mailchimp.com
Phone: +1 (844) 535-0069

- **Description of the processing:**
  Mailchimp is used for email communication and marketing campaigns. Mailchimp handles user email storage, segmentation for communication purposes, and the sending of automated marketing or service-related emails. Raterware manages the content and timing of these communications, while Mailchimp ensures secure data transmission and compliance with email marketing laws (CAN-SPAM, GDPR).

---

5. **5. Name: GitHub**

- **Address:** 88 Colin P Kelly Jr St, San Francisco, CA 94107, United States
- **Contact person's name, position, and contact details:**
  Name: GitHub Support
  Email: support@github.com
  Phone: N/A (support via online ticketing system)
- **Description of the processing:**
  GitHub is used for code repository hosting and version control for Raterware's development. GitHub manages the storage, versioning, and access to the codebase. It is responsible for repository security, while Raterware handles the development process and decides who has access to the code.

---

6. **6. Name: Papertrail (a service of SolarWinds)**

- **Address:** 7171 Southwest Parkway, Building 400, Austin, TX 78735, United States
- **Contact person's name, position, and contact details:**

  Name: Papertrail Support
  Email: support@papertrailapp.com
  Phone: +1 (512) 682-9300
- **Description of the processing:**
  Papertrail provides real-time log management for monitoring and troubleshooting Raterware's application and infrastructure. It collects and stores system logs, including logs related to application errors, access control events, and performance monitoring. These logs are securely transmitted from Heroku to Papertrail, where they are encrypted in transit and stored for analysis. Papertrail assists in operational monitoring and incident response, while Raterware controls access to these logs and ensures compliance with data retention and security policies.