IMPORANT NOTE:
PLEASE READ THIS DATA PROCESSING AGREEMENT ("DPA") CAREFULLY BEFORE USING THE EXALATE SOFTWARE ("SOFTWARE"). THIS DPA IS AN INTEGRAL PART OF THE EULA AND AN AGREEMENT BETWEEN YOU ("LICENSEE") AND EXALATE ("LICENSOR" OR "EXALATE"). BY DOWNLOADING, INSTALLING, COPYING, ACCESSING OR OTHERWISE USING THE SOFTWARE LICENSEE, OR THE PERSON OR ENTITY ON BEHALF OF WHICH THE INDIVIDUAL INSTALLING THE SOFTWARE IS ACTING, UNCONDITIONALLY AGREES TO THE TERMS OF THIS DPA. CLICK ON THE "ACCEPT" BUTTON TO ACCEPT ALL THE TERMS AND CONDITIONS OF THIS DPA. IF YOU DO NOT WANT TO BE BOUND BY THIS DPA YOU SHALL NOT BE ABLE NOR ENTITLED TO DOWNLOAD, INSTALL, COPY, ACCESS OR OTHERWISE USE THE SOFTWARE.

DATA PROCESSING AGREEMENT

About this Data Processing Agreement

This Data Processor Agreement supersedes and replaces all previous agreements made in respect of Processing Personal Data and data protection. Parties agree that Exalate is a Processor and the Licensee is a Controller in respect of all Software provided by Exalate related to the Agreement. The aforementioned indication of the Parties as Controller and Processor is consistent with the terms and definitions given within the GDPR. In the provision of the Software related to the Agreement, the Processor will receive and process Personal Data for the benefit of the Controller and according to its instructions and purpose. Specific legislation applies to such Processing. The legislation applicable to these Processing activities includes, among others the GDPR with possible Belgian implementing laws. By means of this Data Processor Agreement (hereafter the "DPA") Parties wish to lay down their specific agreements in respect to Processing Personal Data within the framework of the Agreement.

1. Definitions

Regarding the interpretation of this DPA, the definitions as concluded in the Agreement and in the GDPR will also apply to this DPA, unless this DPA expressly deviates from those definitions.

"Agreement" means the agreement between the Licensee and Exalate pursuant to which the Licensee obtains a right to use the Software, including but not limited to the applicable order form, EULA, terms and conditions and such other documents executed between the Parties.

"Controller" or "Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data (i.e. the Licensee);

"(Personal) Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

"Data Subject" a natural person who is identified or identifiable by the Personal Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"GDPR" Regulation (EU) 2016/679 of the European Parliament and of 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, and repealing Directive 95/46/EC (General Data Protection Regulation);

"Personal Data" means any information relating to an identified or identifiable natural person as defined in the GDPR;

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller (i.e. Exalate);

"Sub-Processor": refers to any third party that is involved in the Processing of Personal Data by the Processor;

"Supervisory Authority": refers independent government body who is responsible for monitoring the application of GDPR;

"Third Party": a natural or legal person, a government agency, a service or other body, not being the Data Subject, neither the Controller nor the Processor, nor the persons authorized under direct authority of the Controller or the Processor to process the Personal Data;

2. Object of this DPA

2.1 This DPA determines the conditions of the Processing by the Processor, on a self-employed basis, of the Personal Data communicated by or at the initiative of the Controller and in the context of the Agreement; this Processing will exclusively take place for the benefit of the Controller and for the purpose as defined by the Controller.

2.2 The nature and purpose of the Processing, the type of Personal Data as well as the categories of the Data Subjects, taking into account the services to be performed, are specified in the data processing details attached hereto in annex A**.**

2.3 The Processor will only process the Personal Data according to the documented instructions of the Controller, and will not use these Personal Data for its own purpose.

2.4 If the Processor is legally obliged to proceed with any Processing of Personal Data, the Processor, unless this would violate applicable mandatory rules, will inform the Controller of such obligation.

3. Compliance with Data Protection Regulations

The Controller and the Processor are obliged to comply with their obligations under applicable legislation (but possibly also codes of conduct, standard contractual clauses, other related regulations).

4. Term

4.1 This DPA is applicable to every Processing of Personal Data executed in the context of the Agreement.

4.2 This DPA applies as long as the Processor processes Personal Data made available by the Controller in the context of the Agreement. This DPA ends automatically upon termination of the Agreement. tThe provisions of this DPA that are either expressly or implicitly (given their nature) intended to have effect after termination of the DPA shall survive the end of the Agreement as regards the Personal Data communicated by or at the initiative of the Controller in the context of the Agreement.

5. Technical and organizational protection measures

The Processor and Controller offer adequate guarantees with regard to the implementation of appropriate technical and organizational measures so that the Processing complies with GDPR requirements and that the protection of the Data Subject's rights is guaranteed.

6. Records of processing activities

Each Party and, where applicable, their representatives, shall maintain a register of the Processing activities under their responsibility. Each such register shall contain at least all legally required data.

7. Data Protection Officer

If required by law, the Controller and/or the Processor will appoint a Data Protection Officer. The contact details of the Data Protection Officer (or any other person responsible for privacy related matters) are the following: dpo@exalate.com

8. Storage of Personal Data

8.1 The Processor will not keep the Personal Data any longer than as required for Processing of such Personal Data in the context of the Agreement. The Controller will not instruct the Processor to store any Personal Data longer than necessary. The storage period will be equal to the term of the Agreement, unless otherwise agreed between Parties.
8.2 Unless storage of the Personal Data is mandatory under Union or Member State law, the Processor shall, within a reasonable period after the end of the Processing services, at the option of the Controller, either erase all Personal Data or return it to the Controller and delete existing copies.

9. Security

9.1 The Controller and the Processor shall take all appropriate technical and organizational measures as referred to in Article 32 GDPR to ensure a level of security appropriate to the risk. The measures taken by the Processor are described in Annex C.
9.2 The Processor shall, taking into account the nature of the Processing and the information available, assist the Controller in ensuring compliance with the obligations resulting from Articles 32 to 36 GDPR. The Controller will reimburse the Processor for services rendered in the context of providing assistance in fulfilling the aforementioned obligations according to Article 17 “Costs” of this DPA.
9.3 Only those agents of the Processor who are involved in the Processing of Personal Data may be informed about the Personal Data. The Processor ensures that persons authorized to process the Personal Data are committed to confidentiality by contract or are under an appropriate statutory obligation of confidentiality.
9.4 The Processor may only provide Personal Data to Third Parties with the prior written approval of the Controller.

10. Code of Conduct and Certification

Adherence by the Processor to an approved code of conduct as referred to in Article 40 GDPR, or an approved certification mechanism as referred to in Article 42 GDPR may be used as an element of proof of sufficient guarantees as referred to in GDPR.

11. Data Subject’s rights

11.1 Taking into account the nature of the Processing, the Processor shall use best efforts, by taking appropriate technical and organizational, to assist the Controller in the fulfillment of its obligation to respond to requests from Data Subjects.
11.2 For all services performed by the Processor in the context of the treatment of such requests from Data Subjects, the Controller will pay the Processor in accordance with Article 17 “Costs” of this DPA.

12. Duty to notify

12.1 Upon becoming aware of a Personal Data Breach the Processor shall notify the Controller thereof without undue delay.
12.2 At the request of the Controller, the Processor will cooperate with the investigation and elaboration of the measures necessary in case of any Personal Data Breaches.
12.3 The Parties will keep each other informed of any new developments with regard to any Personal Data Breach and of the measures they take to limit its consequences and to prevent the repetition of such Personal Data Breach.
12.4 It is the responsibility of the Controller to report any Personal Data Breach to the Supervisory Authority or the Data Subject, as required.

13. Sub-processing

13.1 The Controller expressly authorizes the Processor to engage Sub-Processors for the processing of Personal Data. The Controller grants a proxy to the Processor to decide with which Sub-Processors the Processor cooperates. The Processor shall keep a list of all Sub-Sub-Processors engaged, which can be consulted by the Controller upon simple request. The current list of Sub-Processors is added in Annex B to this DPA. The Controller can only refuse a Sub-Processor proposed by the Processor on the basis of a well-founded justification submitted in writing.
13.2 The Processor will conclude a separate subcontracting agreement with each Sub-Processor.
13.3 In this subcontracting agreement, substantially the same data protection obligations as set out in this DPA shall be imposed on the Sub-Processor.
13.4 In the event the Sub-Processor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the obligations of that Sub-Processor in accordance with Article 19 of this DPA.

14. Transfers of Personal Data

14.1 The Processing of Personal Data will take place within the European Economic Area (EEA), except as otherwise specified in Annex B.
14.2 The Processing or transfer of Personal Data outside the EEA can occur in compliance with applicable legislation. The Processor can sign standard contractual clauses, codes of conduct or any other instruments adopted by the European Commission, which ensures that the transfer of Personal Data to a country outside the EEA complies with appropriate safeguards as required by the GDPR.

15. Data Protection Impact Assessment

15.1 When a 'Data Protection Impact Assessment' or a 'prior consultation' is required according to Article 35 and 36 GDPR, the Controller will implement such assessment. At the request of the Controller, the Processor will assist in this assessment as well as in the compliance with any required measures.
15.2 The Controller will reimburse the Processor for the services so rendered in relation to this assessment and the compliance with any required measures in accordance with Article 17 "Costs" of this DPA.

16. Audit – inspection

16.1 Each Party shall allow the other Party and its authorized auditors to perform audits regarding the compliance by a Party with its obligations under this DPA and the applicable legislation in respect of data protection.
16.2 Each Party shall use its best efforts to cooperate with those audits and to make available to the other Party all information necessary to prove compliance with the obligations of such Party. A Party shall immediately inform the other Party if, in its opinion, an instruction infringes the applicable legislation. In case the audit required more than one business day of services of the Party which is being audited, the auditing Party will compensate the services provided on a time and material basis (at standard rates applicable at that moment in time).
16.3 Upon the performance of any such audit, the confidentiality obligations of the Parties with respect to Third Parties must be taken into account. Both the Parties and their auditors must keep the information collected in connection with an audit secret and use it exclusively to verify the compliance by the other Party with this DPA and the applicable laws and regulations in respect of data protection.
16.4 The Controller and the Processor and where applicable their representatives, shall cooperate, upon request, with the Supervisory Authority in the performance of its tasks.

17. Costs

17.1 The services to be performed under this Agreement for which the Processor may charge the Controller, will be charged on the basis of the hours worked and the applicable standard hourly rates of the Processor. The Processor will invoice these amounts on a monthly basis.
17.2 Payment by the Controller to the Processor for the services under this Agreement will take place in accordance with the provisions in the Agreement.

18. Notice of default

When the Processor fails to comply with its obligations under this DPA, the Controller shall first send a registered notice of default. This notice shall clearly mention the defaults that occurred, and, if redress is possible, a proposal of remedial measures and a reasonable term for their implementation.

19. Liability

19.1 Limitations of liability in the Agreement are applicable to this DPA and all services provided in respect of this DPA.
19.2 The Processor is in any case only liable for the damage caused by Processing if it (a) did not comply with its specific obligations of the GDPR, or (b) acted outside or in violation of the lawful instructions of the Controller.

20. Other provisions

The provisions of the Agreement concerning changes, completeness of the agreement, applicable law and competent court are applicable to this DPA

Annex A – Description of Processing

Subject Matter	Exalate provision of the services (as described in the Agreement) to the Controller
Categories of Data Subjects Whose Personal Data is Processed	Personal Data of following categories of Data Subjects may be Processed: 1. Website visitors & Users of the Software 2. Such categories of Data Subjects that are included in the data that will be synchronized between various work management tools by making use of the Software (as configured by the Licensee).
Categories of Personal Data Processed	Following categories of Personal Data may be Processed: • Personal identifiers: name, email, telephone • Professional data: company name, company domain • Electronic identifiers: Device ID, IP address, Tracking ID • Usage data for Exalate nodes deployed on Exalate cloud • Such categories of Personal Data that are included in the data that will be synchronized between various work management tools by making use of the Software (as configured by the Licensee).
Sensitive Data Transferred	Depending on how the Licensee has configured the Software, data processed by the Software may be sensitive data (such as medical data).
Nature and Purposes of the Processing	• Providing a platform that acts as a middleware to transfer data between work management tools, without the capability to store personal data as separate data entities. • Communicating with users on the Exalate and Exalate websites or email (including helpdesk) • Reporting on the usage of the product
Period for which the Personal Data will be Retained	180 days after archiving of Exalate node.
Transfers to Sub-Processors	As set out in Annex B

Annex B - List of Sub-Processors

Name	Address	Contact details	Description of Processing	Entity HQ	Data Processing Location
Google LLC	1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Privacy Help Center	Web Analytics Cloud hosting Google Workspace for email and productivity tasks	US	Europe
Rsync.net	524 San Anselmo Ave. Suite 107 San Anselmo, CA 94960 USA	John Kozubik John.kozubik@rsync.net	Storage of encrypted off site backup data	US	CH
Cellnex	Papendorpseweg 75 - 79, 3528 BJ Utrecht, Netherlands	info@cellnextelecom.nl	Colocation datacenter	ES	NL
LCL	Kouterveldstraat 13, 1831 Machelen Belgium	info@lcl.be	Colocation datacenter	BE	BE
DCU	Noorderlaan 147, 2030 Antwerpen Belgium	hello@datacenterunited.com	Colocation datacenter	BE	BE

Annex C – Description of Technical and Organisational Measures

Measures of pseudonymization and encryption of personal data

All communication between users and our application are secured with 128-bit TLS 1.2 encryption and above. All databases and backups are encrypted at rest with AES-256. When a user deletes or requests us to delete their user account we replace personal identifiable information with a nil value.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Data is separated per tenant. Our organization's development and production environments are fully separated. All relevant employees have undergone background screening. All employees, independent contractors and subcontractors are required to execute a confidentiality agreement. All employees and independent contractors receive security awareness training on the Security Policy in place. Disciplinary action might occur in the event policies are neglected. An asset management policy is in place including a disposal policy. Information assets are classified and protected according to their label. All Exalate endpoints are centrally managed: automatic device locking, automatic password policy enforcement, automatic software roll-out, remote wiping in case of stolen or damaged equipment, protected with anti-malware software and data loss protection and data is transferred securely. Our networks are protected with multiple layers of controls (firewall, virus scanner, watchful monitoring, etc.).

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

We backup all data on a daily basis with a 2-day retention period. We have established a Business Continuity Plan to recover the IT systems in case of a disruptive incident and to provide user access to them.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Annual periodic penetration testing by an independent external party is used to audit application and server security. For continuous feedback from the security community a bug bounty program is set up via the BugCrowd platform.

Measures for user identification and authorization

All account passwords are protected irreversibly. Employees cannot reconstruct passwords in any way or form. We have set strong password requirements. Employee access to our infrastructure is strictly limited to engineers who require such access in order to maintain the stability and efficiency of our systems. Access is based upon the principles of least privilege, need to know and need to use and it requires the use of two-factor authentication. We ensure on-going management of system access.

Measures for the protection of data during transmission

All communication between users and our application are secured with 128-bit TLS 1.2 encryption and above. The organization-provided electronic messaging facilities must always be used when communicating with others on official business.

Measures for the protection of data during storage

All databases and backups are encrypted at rest with AES-256. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, biometric locks, and other electronic means. Only authorized personnel have access to the data centers. We have put in place a Cloud Computing Policy to establish rules for the selection and management of cloud computing services so that data is appropriately protected.

Measures for ensuring physical security of locations at which personal data are processed

Being a geographically distributed company with employees working in home offices or public co-working spaces, Exalate's information security strategy is to focus on the endpoints and cloud services rather than building bastion locations. However, all our office spaces meet local building regulations and have lockable doors to prevent theft. All offices require badge-based access to enter.

Measures for ensuring events logging

Advanced user-, file- and network-activity anomaly detection monitors our infrastructure. All access to servers and hosting providers are monitored. All endpoints, servers and other equipment (such as network routers and switches) involved in hosting the storage or processing of classified information have the available audit logging facilities activated to allow the recording and monitoring of activities. Log files will be kept for a period of six months and are internally audited on a regular basis.