



MediusGo Data Processing Addendum

This data processing addendum (the “DPA”) forms part of the agreement between MediusSverige AB and You (the “Agreement”) to reflect the parties agreement with regard to Processing of Personal Data and contains certain terms relating to data protection, privacy, and security in accordance with the requirements of the GDPR, the UK GDPR and the CCPA, where applicable. In the event that there is a conflict between the GDPR, the UK GDPR and the CCPA, the parties shall comply with the more onerous requirement or higher standard. This DPA was last updated on 4 January 2024 and is effective between You and Us as of the date of Your acceptance thereof.

All capitalized terms not defined herein, shall have the meaning set forth in the Agreement.

In the course of providing services to You pursuant to the Agreement, We may process Personal Data on behalf of You and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting in good faith.

1. DEFINITIONS

The following terms shall have the following meanings in this Data Processing Addendum.

- 1.1 “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control”, or purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- 1.2 “**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.
- 1.3 “**CCPA**” means the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 - 1798.199).
- 1.4 “**Data Protection Legislation**” means: i) the GDPR and all other applicable EU, EEA or European single market Member State laws or regulations or any update, amendment or replacement of same that apply to processing of personal data under the Agreement; (ii) all U.S. laws and regulations that apply to processing of personal data under the Agreement including but not limited to CCPA; (iii) all laws and regulations that apply to processing of personal data under the Agreement from time to time in place in the United Kingdom (including the UK GDPR), and the terms “controller”, “process”, “processing”, “processor”, “supervisory authority” have the same meanings as in the GDPR or the UK GDPR and with respect to CCPA (as defined above) as applicable, the Parties hereby agree that We are a “Service Provider” and You are the “Business”, as defined under the CCPA with respect to Personal Information (as defined under the CCPA).
- 1.5 “**Data Subject**” means the identified or identifiable person to whom Personal Data relates.
- 1.6 “**GDPR**” means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation). References in this DPA to GDPR will to the extent applicable be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).
- 1.7 “**Personal Data**” means any information relating to an identified or identifiable natural person where such data is Your data.
- 1.8 “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
- 1.9 “**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automated means (such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use,



disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction).

- 1.10 **“Processor”** means the entity which Processes Personal Data on behalf of the Controller.
- 1.11 **“Restricted Transfer”** means i) a transfer of Personal Data from You to Us or ii) an onward transfer of Personal Data from Us to a Sub-processor, in each case, where such transfer would be prohibited by Data Protection Laws and Regulations in the absence of the Standard Contractual Clauses, the UK Addendum or any other transfer mechanism referenced in chapter 5 of the GDPR. For the avoidance of doubt, where a transfer of Personal Data is of a type authorised by Data Protection Laws or Regulations in the exporting country, for example in the case of transfers from within the European Union to a country (such as Switzerland or the United Kingdom) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer.
- 1.12 **“Services”** means the Services provided to You under the Agreement.
- 1.13 **“Standard Contractual Clauses”** means the Standard Contractual Clauses pursuant to Commission Decision (EU) 2021/914 of 4 June 2021 in conjunction with the International Data Transfer Addendum to the EU Standard Contractual Clauses available at <https://www.medius.com/legal/uk-addendum-to-dpa/> (the **“UK Addendum”**).
- 1.14 **“Sub-processor”** means any Processor engaged by Us or by Our Affiliate/s.
- 1.15 **“Supervisory Authority”** means an independent public authority which is established by an EU Member State pursuant to the GDPR.
- 1.16 **“UK GDPR”** means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).
- 1.17 **“We”/“Us”/“Ours”** and **“Medius”** means the Medius company with which You have entered into the Agreement.
- 1.18 **You”/“Your”/“Yours”** and **“Customer”** means the company or other legal entity that executes the Agreement with Medius.

2. PROCESSING OF PERSONAL DATA

- 2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to Our Processing of Personal Data on Your behalf, You are the Controller and We are the Processor.
- 2.2 **Your Processing of Personal Data.** You shall Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and Your instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. You shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which You collected Personal Data.
- 2.3 **Our Processing of Personal Data.** We shall treat Personal Data as confidential information and shall only Process Personal Data on behalf of and in accordance with Your documented instructions for the following purposes: (a) Processing in accordance with the Agreement; (b) Processing initiated by Users in their use of the Services; and (c) Processing to comply with other documented reasonable instructions provided by You where such instructions are consistent with the terms of the Agreement. We will immediately inform You if any of Your instructions, in Our opinion, infringes any Data Protection Laws and Regulations. We shall be responsible for complying with all Data Protection Laws applicable to Our provision of the Services in Our role as Data Processor. However, we are not responsible for compliance with any laws applicable to Your or Your industry that are not generally applicable to information technology service providers. To the extent We will process Your data that is “Personal Information” subject to the CCPA, We do so as a service provider (as the term is defined in the CCPA) and acknowledge the following restrictions: a) We will process, retain, use, and disclose personal information, including Customer Data, for the sole purpose of providing the Services or as otherwise permitted under this Agreement; b) We will not process, retain, use, or disclose, including to a third party for valuable consideration, Personal Information, including Customer Data, for any other purpose; c) We will not process, retain, use, or disclose personal information, including Customer Data, for any purpose outside of the direct business relationship between You and Us; and d) We shall provide reasonable support and response to inquiries from You regarding Our data processing obligations.



2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Us is the performance of Services. Details about the duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Appendix 1 (Details of the Processing) to this DPA.

2.5 **Affiliates and third parties.** In case it is expressly agreed under the Agreement that Your Affiliates or any other third parties shall also benefit from the Services, You act in this respect on behalf of and in the name of Your Affiliates and/or third parties in their capacity as Controllers and You shall to the extent necessary enter into data processing agreements with such Controllers required to allow Us and Our Sub-processors to process any Personal Data as described in this DPA. You shall serve as a single point of contact for Us and shall be solely responsible for the internal coordination, review and submission of instructions or requests of other Controllers to Us and We shall be entitled to refuse any requests or instructions provided directly by a Controller that is not You. We shall further have no obligation to inform or notify a Controller when We have provided such information or notice to You.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** We shall, to the extent legally permitted, promptly notify You if We receive a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, We shall assist You by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Your obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent You, in Your use of the Services, do not have the ability to address a Data Subject Request, We shall upon Your request provide commercially reasonable efforts to assist You in responding to such Data Subject Request, to the extent We are legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, You shall be responsible for any costs arising from Our provision of such assistance.

4. SECURITY AND CONFIDENTIALITY

4.1 **Protection of Personal Data.** We shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to Your Personal Data), confidentiality and integrity of Your Personal Data. Such measures shall take into account the nature, scope, context and purposes of the Processing as well as the risks of varying likelihood and severity for the rights and freedom of natural persons. The measures shall be reviewed and updated where necessary.

4.2 **Confidentiality.** We shall ensure that Our personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. We shall take commercially reasonable steps to ensure the reliability of Our personnel engaged in the Processing of Personal Data and shall ensure that Our access to Personal Data is limited to those personnel performing Services.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** You acknowledge and agree that (a) Our Affiliates may be retained as Sub-processors; and (b) We and Our Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services and (c) that We may continue to use those Sub-processors already engaged by Us or Our Affiliates as at the date of this Addendum, which are listed in Schedule A. We or Our Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Addendum with respect to the protection of Your Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. You acknowledge and agree that We may remove Sub-processors at Our own discretion.

5.2 **New Sub-processors.** You may object to Our use of a new Sub-processor by notifying Us in writing within (10) business days after receipt of information of Our intended changes concerning the addition of a new Sub-processor. In the event You object to a new Sub-processor, as permitted in the preceding sentence, We will use reasonable efforts to make available to You a change in the Services or recommend a commercially reasonable change to Your configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening You. If We are unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, You may terminate the Agreement with respect only to those Services which cannot be provided by Us without the use of the objected-to new Sub-processor by providing written notice to Us. We will refund You any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on You.



5.3 **Liability.** We shall be liable for the acts and omissions of Our Sub-processors to the same extent We would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. NOTIFICATION OF PERSONAL DATA BREACHES AND OTHER ASSISTANCE

6.1 We shall notify You without undue delay, and where feasible, not later than 48 hours, after becoming aware of a Personal Data Breach affecting Your Personal Data, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons, providing You with sufficient information to allow You to meet any obligations to report or inform Data Subjects or the Supervisory Authority pursuant to article 33 of GDPR or any other applicable law or regulation to notify relevant supervisory authorities or data subjects. We shall investigate the Personal Data Breach and take reasonable steps to mitigate the effects and to minimize any damage resulting from the breach.

6.2 To the extent not already explicitly covered by Our obligations in this DPA, We shall assist You in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDOR taking into account the nature of processing and the information available to Us.

7. RETURN AND DELETION OF PERSONAL DATA

7.1 Unless otherwise is explicitly agreed in the Agreement, We shall upon the expiration or termination of the Agreement or upon Your request, provide You with your Personal Data in standardized format at Your cost. If You require the data in another format, We undertake to investigate the possibilities to perform such export. We undertake to store the Data one (1) month after the Agreement's expiration or termination or until any requested transfer of data has been performed and the data will be deleted not later than ninety (90) days thereafter.

8. RESTRICTED TRANSFERS

8.1 The Parties understand and agree that Personal Data processed in accordance with this DPA may be transferred to respectively accessed from countries outside of the EU/EEA, the UK, US and Switzerland by Us, Our Affiliates and Sub-processors when providing the Services in accordance with the terms of the Agreement.

8.2 For Restricted Transfers from the European Economic Area that are subject to the Standard Contractual Clauses, We and Our Affiliates and the third party Sub-processors shall execute and adhere to Module Three (Processor to Processor) of the Standard Contractual Clauses. For Restricted Transfers from the UK that are subject to the Standard Contractual Clauses, We and Our Affiliates and the third party Sub-processors shall execute and adhere to Module Three (Processor to Processor) of the Standard Contractual Clauses in conjunction with the UK Addendum. Upon Your request, we shall make information on the transfer, and where applicable, the Standard Contractual Clauses and supplementary measures available to You, without undue delay.

8.3 We will have the right to amend this section 8 in case Standard Contractual Clauses and/or the UK Addendum are amended, revoked or held in a court of competent jurisdiction to be invalid.

8.4 Notwithstanding section 8.2 above, for onward transfers to Sub-processors engaged prior to the effective date of this DPA, We may rely on the standard contractual clauses for the transfer of personal data to processors or sub-processors established in third countries as adopted by the Europe Commission under Directive 95/46/EC: a) until 27 December 2022 with respect to transfers from the European Economic Area and b) until 21 March 2024 with respect to transfers from the UK.

9. AUDIT

9.1 We will on a regular basis audit the security measures taken by Us to protect Your data, including Personal Data, when providing the Services. Upon Your written request, We will provide You with a confidential summary of the result of such audit, for instance in the form of a SOC report, to allow for You to verify Our compliance with Our security obligations set out in this DPA. The report is Our confidential information and is protected by the confidentiality clause set forth in the Agreement.

9.2 You agree to exercise Your audit right by instruction Us to execute the audit as described in section 9.1. If You reasonably concludes that the provision of Our audit report is not sufficient to demonstrate Our compliance with this DPA, We and Our Affiliates shall, subject to section 9.3, make available to You on request all information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits, including inspections, by You or an auditor mandated by You in relation to the Processing of Your Personal Data by Us. Information and audit rights of You only arise to the extent that the

Agreement does not otherwise give You information and audit rights meeting the relevant requirements of Data Protection Laws and Regulations (including, where applicable, article 28(3)(h) of the GDPR).

- 9.3** You shall give Us reasonable notice of any audit or inspection to be conducted under section 9.2 and shall make (and ensure that each of Your mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the audited premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. We do not have to give access to premises for the purposes of such an audit or inspection outside normal business hours at those premises, or for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which You are required or requested to carry out by Data Protection Laws and Regulations or a Supervisory Authority.

10. LIABILITY

- 10.1** The parties' liability under this DPA shall be subject to the same limitation of liability as agreed between the Parties in the Agreement.
- 10.2** Nothing in this DPA or Agreement relieves either Party of its own direct responsibilities and liabilities under Data Protection Laws and Regulations.

11 MISCELLANEOUS

- 11.1** Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses, the parties of this DPA hereby submits to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA.
- 11.2** Nothing in this DPA reduces Our obligations under the Agreement in relation to the protection of Personal Data or permits Us to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses in conjunction with the UK Addendum shall prevail. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.
- 11.3** Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.



IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the date set out below. Notwithstanding the foregoing, if this DPA is entered into simultaneously with the Agreement, this DPA will become a binding part of the Agreement with effect from the date the Agreement is signed and this DPA does not have to be separately signed.

Customer name _____

Signature _____

Name _____

Title _____

Date Signed _____

Medius entity

Signature _____

Name _____

Title _____

Date Signed _____



APPENDIX 1

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

1. Data subjects

You may submit Personal Data to Us, the extent of which is determined and controlled by the You in Your sole discretion, and which may include but is not limited to Personal Data relating to the following categories of data subjects:

- Your Employees, consultants or other representatives
- Your Users of the Services
- Invoice contact persons of Your suppliers and other individuals referenced on invoices
- Representatives of Your suppliers.
- Individuals referenced on contracts processed for signature via the Services.
- Your and Your contractual counterparty's signatories.

2. Categories of data

You may submit Personal Data to Us, the extent of which is determined and controlled by the You in Your sole discretion, and which may include but is not limited to the following categories of Personal Data:

- First and Last name
- Title
- Contact information (company, email, phone, address)
- User ID
- Any information referenced in invoices or in contracts processed via the Services.
- IP number
- Bank account details

3. Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

- N/A, unless defined by You.

4. Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data is to provide, maintain and develop the Services pursuant to the Agreement.

5. Duration

As requested by You – however no longer than for the duration of the Agreement plus the period from the termination of the Agreement until deletion of Your data in accordance with the Agreement.

APPENDIX 2

(Description of the technical and organisational security measures implemented by the data importer)

Medius maintains security measures appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. These measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected, taking into account the state of the art and the cost of implementation. The measures are subject to technical progress and development and We are therefore expressly allowed to implement adequate alternative measures as long as the general security level described in this appendix 2 is maintained.

The technical and organisational security measures that Medius currently has in place for any system that processes Personal Data with regard to prevent improper destruction, alteration, disclosure, access, and other improper forms of processing of information exported by the data exporter to the data importer, include the following areas:

- Access control
- Information Classification (and handling)
- Physical and Environmental Security
- Acceptable Use of Assets
- Clear Desk and Clear Screen
- Information Transfer
- Mobile Device and Teleworking
- Restrictions on Software Installation and Use
- Backup Routines
- Malware-protection
- Management of Technical Vulnerabilities
- Cryptographic Controls
- Communications Security
- Privacy and Protection of Personally Identifiable Information
- Subcontractor Relationship



SCHEDULE A

LIST OF SUB-PROCESSORS

The parties below or their subsidiaries may provide services to one or more Services offered under the Agreement.

Subprocessor	Location	Comment/Nature of the processing
Medius Aps, Medius Business Process Software BV, Medius AS, Medius Sverige AB, Medius Poland Sp. Z.o.o., Dynamic Software in Sweden AB, Expensya SA	EU	Medius affiliates
Medius Software Ltd	UK	Medius affiliate
Medius Software Pty Ltd	Australia	Medius affiliate
Medius Software Inc and OnPay Solutions Inc	USA	Medius affiliate
Expensya Sarl	Tunisia	Medius affiliate
Microsoft Ireland Operations Limited	EU, USA, UK or Australia (follows customer primary location, except Azure AD user transfer services that are operated from EU)	Provider of the cloud hosting platform (Azure).
Microsoft Ireland Operations Limited	EU or USA (follows customer primary location)	Exchange Online (e-mail delivery service) for capture.
Sendgrid Inc	USA	E-mail delivery services
Papertrail Inc	USA	Log handling
Kofax Sweden Technologies AB	EU, USA or Australia (follows customer primary location)	Capture services (provider of ReadSoft Online)
Abby Europe GmbH	EU or USA (follows customer location)	Capture services
Freshworks Inc	EU	System to manage support requests from Medius' users
SolarWinds Worldwide LLC	USA	Log handling (Loggly)
CDC Arkhineo	EU	Provider of Archiving solution for expense management services
Atea Sverige AB	Sweden	Provider of the MediusGo service infrastructure
Webbkonsulterna AB	Sweden	E-mail delivery service
Inexchange Factorum AB	Sweden	Where the provision of Scancloud services is part of the Agreement



Attest.nu i Sverige AB	Sweden	Where the Attest.nu service is part of the Agreement
Exela Technologies AB	Sweden	Where the Exela service is part of the Agreement
Companyexpense Svenska AB	Sweden	Provider of Company Expense service