CRONOFY – DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") forms part of the subscription agreement, Cronofy's Terms of Service available at https://www.cronofy.com/terms-of-service/ or other written or electronic agreement (the "Agreement") entered into between Cronofy and Subscriber, pursuant to which Cronofy provides Services as defined in the Agreement. This DPA is based on, and in line with, the standard contractual clauses as published by the European Commission.[1]

The purpose of this DPA is to reflect the parties' agreement with regard to the processing of Subscriber Personal Data. The parties agree to comply with this DPA with respect to any Subscriber Personal Data that the Cronofy may process in the course of providing the Services pursuant to the Agreement. This DPA shall not replace or supersede any data processing addendum or agreement executed by the parties prior to the DPA Effective Date without the prior written consent of the parties (electronically submitted consent acceptable).

This DPA will take effect on the DPA Effective Date and, notwithstanding expiry of the Term, will remain in effect until, and automatically expire upon, deletion of all Subscriber Data by Cronofy as described in this DPA.

If the Subscriber entity entering into or accepting this DPA is neither a party to a Service Order nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Subscriber entity that is a party to the Agreement executes this DPA.

SECTION I

Clause 1

Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
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) of 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.

[1] COMMISSION IMPLEMENTING DECISION (EU) 2021/915 of 4 June 2021 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

Clause 5 - Optional

Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

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) 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 two months 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.

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 [OPTION 1] Article 32 of 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 of Regulation (EU) 2016/679 or under Articles 34 and 35 of 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) of 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 of 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 1 - List of Parties

Controller		**Processor**	
Signature	Matthias Blenski	Signature	DocuSigned by: Karl Bagci 5298882492D7408...
Date	02 / 24 / 2022	Date	08-Dec-2021
Name	Matthias Blenski	Name	Karl Bagci
Position	Syndikusanwalt	Position	Head of Operations
Company	d.vinci HR-Systems	Company	Cronofy B.V.
Address	Nagelsweg, Hamburg	Address	Appollolaan 151, Amsterdam

ANNEX 2 - Description of Processing

Processor

The processor is a Software-as-a-Service API provider who offers a platform for software providers to interact with end-user and organizational calendars. This involves securely handling credentials for access to calendar data as well as the calendar data itself. The processor will have access to any data provided by the controller. This will be used exclusively to provide service to the controller. The processor will also provide the controller access to end-user and organizational calendar data subject to the authority granted by the end-user or organizational authority.

Data subjects

The personal data processed concern the following categories of data subjects:

End users of the Service; and

End users to whom Controller`s Customer provide access to the Service (including Controller's Customers` employees and contractors)

Categories of data

The personal data processed concern the following categories of data:

Email addresses; calendar structures; subject, location and timings of calendar events.

Special categories of data

The personal data processed concern the following special categories of data:

None

Processing operations

The personal data processed will be subject to the following basic processing activities:

Data will be transferred between the controller and the processor via encrypted API communication protocols. As part of the standard operating model of the service, calendar and event data is stored in databases. The trigger for storing this information is the controler being granted authority by the end-user or organizational authority to access the data. When that authority is terminated this data is removed according to the following standard policy:

30 days after authorization terminated
- Tokens/credentials deleted
- Third party events (sourced from user's calendars)
- Stop syncing

90 days after authorization terminated
- Partner events (calendar events generated by the data exporter)
- Calendar structure

Partner events exist in API journals which are kept as archive for up to 90 days.

ANNEX 3 – Technical and organizational measures, including technical and organizational measures to ensure the security of data

Cronofy may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services. These Security Measures are in effect on the DPA Effective Date. Capitalized terms used herein but not otherwise defined have the meaning given to them in the DPA.

Information Security Program

1. **Data Centres and Network Security**
   a. **Data Centres**
      i. **Infrastructure.** Cronofy maintains geographically distributed data centres and stores all production data in physically secure data centres.
      ii. **Redundancy.** Cronofy's infrastructure has been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. This design allows Cronofy to perform maintenance and improvements of the infrastructure with minimal impact on the production systems. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications.
      iii. **Power.** All data centres are equipped with redundant power system with various mechanism to provide backup power, such as uninterruptible power supplies (UPS) batteries for short term blackouts, over voltage, under voltage or any power instabilities and diesel generators, for outages extending units of minutes, which allow the data centres to operate for days.
      iv. **Server Operating System.** Cronofy uses a Linux based operating system for the application environment. Cronofy has established a policy to keep systems up to date with necessary security updates.
      v. **Business Continuity.** Cronofy replicates data across multiple systems to help protect against accidental destruction or loss. Cronofy has designed and regularly plans and tests its business continuity planning and disaster recovery programs.
   b. **Network and Transmission**
      i. **Data Transmission.** Cronofy uses industry standard encryption schemes and protocols to encrypt data transmissions between the data centres. This is intended to prevent reading, copying or modification of the data.
      ii. **Incident Response.** Cronofy's security personnel will promptly react to discovered security incidents and inform the involved parties.
      iii. **Encryption Technologies.** Cronofy's servers support HTTPS encryption, ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA and for supported clients also perfect forward secrecy (PFS) methods to help protect traffic against compromised key or cryptographic breakthrough. Cronofy uses only industry-standard encryption technologies.
2. **Access and Site Controls**
   a. **Site Controls**
      i. **Data centre Security Operations.** All data centres in use by Cronofy maintain 24/7 on-site security operations responsible for all the aspects of physical data centre security.
      ii. **Data centre Access Procedures.** Access to the data centre follows Cronofy's Physical Security policy allowing only pre-approved authorized personnel to access Cronofy's equipment.
      iii. **Data centre Security.** All data centres comply with or exceed the security requirements of SOC2. All data centres are equipped with CCTV, on-site security personnel and key card access system.
   b. **Access Control**
      i. **Access Control and Privilege Management.** Subscriber's administrators must authenticate themselves in order to administer the Services.
      ii. **Internal Data Access Processes and Policies – Access Policy.** Cronofy's internal data access processes and policies are designed to prevent unauthorized persons or systems from getting access to system used to process personal data. Cronofy employs a centralized access management system to control access to production systems and server, and only provides access to a limited number of authorized personnel. SSO, LDAP and SSH certificates are used to provide secure access mechanisms. Cronofy requires the use of unique IDs, strong passwords and two factor authentication. Granting of access is guided by an internal policy.
3. **Data**
   a. **Data Storage, Isolation and Logging.** Cronofy stores data in a combination of dedicated and multi-tenant environment on Cronofy-controlled servers. The data is replicated on multiple redundant systems. Cronofy also logically isolates the Subscriber's data. Subscriber may enable data sharing, should the Services functionality allow it. Subscriber may choose to make use of certain logging capability that Cronofy may make available via the Services.
   b. **Decommissioned Disks and Disk Erase Policy.** Disks used in servers might experience hardware failures, performance issue or errors that lead to their decommission. All decommissioned disk are securely erased if intended for reuse, or securely destroyed due to malfunction.
4. **Personnel Security**
   a. Cronofy personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Cronofy conducts appropriate backgrounds checks to the extent allowed by applicable law and regulations.
   b. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Cronofy's confidentiality, privacy and acceptable use policies. All personnel are provided with security training upon employment and then regularly afterwards. Cronofy's personnel will not process Subscriber Data without authorization.

5. **Sub-processor Security**

a. Cronofy conducts audit of security and privacy practices of Sub-processors prior to onboarding the Sub-processors in order to ensure adequate level of security and privacy to data and scope of services they are engaged to provide. Once the Sub-processor audit is performed and associated risk is evaluated, the Sub-processor enters into appropriate privacy, confidentiality and security contract terms.

ANNEX 4 - Sub-processors

The processor currently works with the following subcontractors in order to perform the commissioned duties. The controller agrees upon their engagement pursuant to clause 7.7.a. The sub-processors utilized depend on the data centre chosen when setting up the application with Cronofy, by the controller.

a. Infrastructure Sub-processors

Cronofy operates worldwide infrastructure using leading cloud service providers. Cronofy owns and controls logical access to the infrastructure maintained by the entities set forth below, while these entities maintain the physical security of the servers, network and the data centre.

Data centre	**Service Provider**	**Infrastructure Location**
US (default)	Amazon Web Services Inc.	United States
DE	Amazon Web Services Inc.	Germany
UK	Amazon Web Services Inc.	United Kingdom
AU	Amazon Web Services Inc.	Australia
SG	Amazon Web Services Inc.	Singapore
CA	Amazon Web Services Inc.	Canada

b. Service Sub-processors

Cronofy utilises specialist service providers to deliver aspects of the service. The service providers utilized depend on the data centre choice by the Controller.

US (default) Data centre

Service Provider	**Service Location**	**Primary Service Type**
Amazon Web Services Inc	United States	Database
Airbrake	United States	System log alerting

DE Data centre

Service Provider	**Service Location**	**Primary Service Type**
Amazon Web Services Inc	Germany	Database

UK Data centre

Service Provider	**Service Location**	**Primary Service Type**
Amazon Web Services Inc	United Kingdom	Database

AU Data centre

Service Provider	**Service Location**	**Primary Service Type**
Amazon Web Services Inc	Australia	Database

SG Data centre

Service Provider	**Service Location**	**Primary Service Type**
Amazon Web Services Inc	Singapore	Database

CA Data centre

Service Provider	**Service Location**	**Primary Service Type**
Amazon Web Services Inc	Canada	Database

Cronofy UK

Service Provider	**Service Location**	**Primary Service Type**
Cronofy UK	United Kingdom	Business support Finance Support Engineering Sales Success

HELLOSIGN

Audit Trail

TITLE	[Cronofy] - [Cronofy DPA - 2021-12]
FILE NAME	ActiveStorage-105...0124-4-cmwpxf.pdf
DOCUMENT ID	27ebf92bfa1004c3749a09bf36b42ecf2c1ed7da
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Signed

This document was signed on my.pima.app

Document History

SENT	**02 / 24 / 2022** 00:13:35 UTC-8	Sent for signature to Matthias Blenski (matthias.blenski@dvinci.de) from signature@pima.app IP: 100.24.23.253
VIEWED	**02 / 24 / 2022** 00:13:40 UTC-8	Viewed by Matthias Blenski (matthias.blenski@dvinci.de) IP: 193.27.46.241
SIGNED	**02 / 24 / 2022** 00:18:58 UTC-8	Signed by Matthias Blenski (matthias.blenski@dvinci.de) IP: 193.27.46.241
COMPLETED	**02 / 24 / 2022** 00:18:58 UTC-8	The document has been completed.