In this 2tCloud Processor Agreement (PA), definitions, words or phrases will have the same meaning as in the Cloud Partner Agreement respectively the Cloud End User Agreement, unless and to the extent the context requires otherwise.

This PA is entered into between Customer (acting as the Data Controller) and the Partner (acting as the Data Processor).

# Article 1 Background

1.1 Customer and Partner acknowledge that the Cloud Services may imply the processing of Personally Identifiable Information (Personal Data) on the Platform such as:

i. Company Name;

ii. Tax Registration ID (VAT);

iii. Company Postal Address; Address; City; Postal Code; Country;

iv. Administrative Contact Information: First Name; Middle Name; Last Name; E-mail; Phone Number; Fax Number;

v. Billing Contact Information: First Name; Middle Name; Last Name; E-mail; Phone Number; Fax Number;

vi. Technical Contact Information: First Name; Middle Name; Last Name; E-mail; Phone Number; Fax Number;

vii. Blind Carbon Copy E-mail;

viii. Bank Account Number;

ix. BIC (Bank Identifier Code);

x. IBAN (International Bank Account Number);

xi. Chamber of Commerce registration number;

xii. User Login to Customer's Control Panel: Name; E-mail; Address; City; Country; Phone Number; Fax Number;

xiii. Domain name and registrar information;

xiv. IP addresses;

xv. The content of virtual servers used by Customer, including but not limited to (confidential) Customer client data. Customer client data may include similar data as included under i to xiv above;

1.2 Customer hereby instructs Partner to Process the Personal Data for the following purposes: (i) Processing in accordance with the Cloud End User Agreement; (i) Processing to comply with any further reasonable instructions of Customer (such as but not limited to instructions via e-mail), when these instructions are in accordance with the Cloud End User Agreement.

1.3 The Customer determines the purpose of the processing of Personal Data on the Platform and has freely decided to use the Cloud Services offered by Partner as part of Customer's IT environment.

1.4 The Customer enters into this PA with Partner to enable Customer to ensure that all processing of Personal Data that takes place as a result of the performance of Cloud Services by Partner for Customer, is in compliance with relevant data protection laws.

# Article 2 General

Partner shall process Personal Data in accordance with the requirements of all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, applicable to the processing of personal data, including but not limited to the Dutch Data Protection Act and the upcoming General Data Protection Regulation.

# Article 3 Confidentiality

3.1 Partner shall keep all Personal Data strictly confidential, make sure that the amount of Officers having access to Personal Data is as limited as possible, and make sure that all Officers having access to Personal Data are bound to the same strict confidentiality obligations.

3.2 Partner is not bound by these confidentiality obligations in case disclosure of Personal Data is required by law, in that case Partner will inform Customer about the disclosure as far as and as soon as legally admitted and reasonably possible.

# Article 4 Security: technical and organizational measures and audit

4.1 As processor, the Partner shall take extensive organizational and technical (security) measures to prevent unauthorized access to Personal Data.

The measures include where appropriate the following measures:

i. All Cloud Services run in Datacenters with Information Security certification and controls ISO27001:2013, ISAE3402 Type II and SOC.

ii. Encryption of Personal Data.

iii. Copaco Personnel must have a Certificate of good conduct;

iv. Protection of network connections;

v. Inbound and Outbound vulnerability assessments;

vi. Vulnerability Intelligence and threat management reporting;

vii. Implemented patch management procedures;

viii. Precautions ensuring that natural persons working for Partner that have access to Personal Data, only process these Personal Data as part of the assignment of Customer, unless such processing would be prescribed by law.

and further measures as described in the Service Level Agreement and the Cloud Services Related Documents.

4.2 Customer has the right to audit these measures in order to assess the adequacy of the measures in relation to the processing and Personal Data at its own costs.

# Article 5 General Information obligations

Partner shall provide a list of locations in which the personal data may be processed.

Partner shall inform the Customer about relevant changes concerning the respective Cloud Services such as the implementation of additional functions.

# Article 6 Rights of data subjects

Partner is obliged to support Customer as far as reasonably possible in facilitating exercise of data subjects' rights to access, correct or delete their data (Personal Data). In case such support would lead to more than negligible costs, these reasonable costs shall be borne by Customer.

# Article 7 Security breaches

7.1 Partner shall implement an appropriate policy with regard to incidents and Security Breaches, such as but not limited to protocols that comply with data protection laws and regulation. A Security Breach is considered any actual or reasonably suspected unauthorized disclosure of Personal Data by Partner or by third parties as appointed by Partner, such as but not limited to Sub-Processors.

7.2 Partner will notify Customer as soon as possible, preferably within 24 (twenty four) hours after the discovery by Partner of any Security Breach or breach of security measures, such as stipulated in article 4.1 above, that leads to the significant chance to severe disadvantageous consequences or severe disadvantageous consequences for the protection of Personal Data and will support Customer in every way possible to handle this breach, such as but not limited to the (support for) a timely notice of the breach to the relevant authorities and, when required, the notification of Data Subjects.

7.3 The notification that Partner makes to Customer as referred to in article 7.2 above, shall as far as reasonably possible entail the following information:

i. The possible cause and consequences of the Security Breach or the incident;

ii. the (categories) of Personal Data involved;

iii. a summary of the possible consequences for Data Subjects;

iv. a summary of the possible (unauthorized) recipients of Personal Data;

v. the measures that Partner recommends to limit the damages, when such is relevant.

7.4 When the notification as referred to in article 7.2 above takes place, Partner will remain available and attainable for consultation with Customer.

# Article 8 Deletion of data

When after the termination of this PA, Partner possesses any Personal Data received from Customer, this Personal Data shall as soon as possible and not later than ten working days after termination of this PA be returned to Customer, or – such in consultation with Customer – be destroyed, save for the situation that Partner is obliged to keep the Personal Data on the basis of applicable laws or regulations. For the interpretation of this article, the possession of Personal Data entails, amongst other definitions but not limited to such, the Personal Data as stored on any data carrier, any rented or bought storage space on servers, whatever the location of such servers, in sandboxes, memory sticks, SSD-cards or any other means that is used to record or store Personal Data.

# Article 9 Sub-Processors

9.1 Customer consents to the use by Partner of Sub-Processors while performing the Cloud Services, and to Partner agreeing with Sub-Processors to use further Sub-Processors as long as 1) these Sub-Processors are bound by similar obligations as Partner under this PA, 2) the Sub-Processors are based in the EU and 3) the Services are performed in the EU. Sub-Processors that may be involved include Copaco Nederland and Copaco Cloud. In case other Sub-Processors are involved, Partner will inform Customer about this, prior to the involvement.

9.2 In principle Personal Data will only be stored within the EU. If it is required to have Personal Data processed outside the EU, Partner shall do so only upon prior written consent by Customer, and shall solely process Personal Data in a country from which the European Commission has determined that such country manages an appropriate level of security for Personal Data, as determined in accordance with Directive 95/46/EG.

9.3 As an exception to the above and only upon prior written consent by Customer, Personal Data may be processed in a country without an appropriate level of security for Personal Data, when this appropriate level of security is ensured in any other way by the appropriate authorities or institutions, such as but not limited to the use of, Binding Corporate Rules (approved by the appropriate authority) or the use of the EU Model Clauses, or other EU approved facilities such as the Privacy Shield Framework. Any Customer consent shall not be unreasonably withheld in case of use of Binding Corporate Rules, EU Model Clauses, or other EU approved facilities such as the Privacy Shield Framework. Customer shall cooperate with concluding standard contracts.

# Article 10 Warranties Customer

Customer warrants that all processing of Personal Data on the Platform on behalf of Customer pursuant to the commission of Customer is in compliance with applicable data protection laws and fully indemnifies Partner against all claims from third parties including Sub-Processors relating to a breach of Data Protection Law by Customer.

# Article 11 Term

This PA will be in force as long as Partner performs Cloud Services for Customer.

# Article 12 Miscellaneous

This PA shall be governed by Dutch law. In case of any conflict with other contractual documents relating to the Cloud Services, this PA will prevail.