28.12.2018

This Analyste personal data processing appendix and its annexes (**"DPA"**) is an appendix to, and legally binding only in connection with, the sales agreement between **Analyste** and **Customer** with regard to Analyste Cloud Services (**"Sales Agreement"**) that references this Appendix. The Sales Agreement, together with all its appendices, is jointly referred to as the "**Agreement**". Capitalized terms used but not defined in this DPA shall have the meaning specified in the Agreement. Any non-capitalized term related to processing of Personal Data (as defined below) used but not defined in this DPA shall have the meaning specified under the applicable data protection law.

1. PREAMBLE

Pursuant to the Agreement, Analyste provides Cloud Services to Customer, as identified in the Sales Agreement. Customer might require Analyste to process Personal Data, on Customer's behalf, for the purpose of providing the Cloud Services.

2. PERSONAL DATA

To the extent Customer requires Analyste to process any information relating to an identified or identifiable natural person on Customer's behalf, in connection with and for the purpose of providing the Cloud Services ("Personal Data"), both parties shall comply with the provisions of this DPA. Personal Data mainly includes, as determined and controlled by Customer in its sole discretion, without being exhaustive, business contact data such as name, title, position, business (email/physical) address, telephone number and language of Customer's and/or Customer's trading partners' individual representatives in the order and/or invoice data that are processed through the Cloud Services. Personal Data may further also include, as determined and controlled by Customer in its sole discretion, special categories of data, which is, for the sake of clarity, Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life or sexual orientation.

3. CUSTOMER OBLIGATIONS

3.1. **Data controller**. Customer shall be the sole data controller for the Personal Data pursuant to the EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "Regulation") and/or any applicable national data protection law and shall be responsible for the lawful collection, processing and use, and for the accuracy of the Personal Data, as well as for preserving the rights of the individuals concerned. If and to the extent legally required, Customer shall inform the individuals concerned regarding the processing of their Personal Data by Analyste, and shall obtain their consent if necessary. Customer acknowledges that due to the nature of the Cloud Services, Analyste cannot control and has no obligation to verify the Personal Data Customer transfers to Analyste for processing on behalf of Customer when Customer uses the Cloud Services. Customer ensures that Customer is entitled to transfer the Personal Data to Analyste so that Analyste may lawfully process the Personal Data on behalf of Customer.

4. ANALYSTE OBLIGATIONS

4.1. **Observe Instructions**. Analyste, being the data processor pursuant to the Regulation, shall, and ensures that its related employees shall, process the Personal Data exclusively on behalf of Customer, as is necessary for Analyste to perform its obligations under the Agreement and in accordance with Customer's Instructions, unless as far as otherwise required by applicable law. Consequently, Analyste shall not use the Personal Data for any other purpose, and shall not transfer the Personal Data to unauthorized third parties, nor use the Personal Data for its own purposes.

4.2. **Assistance**. To respond to requests from individuals exercising their rights as foreseen in applicable data protection law, such as the right of access and the right to rectification or erasure, Customer shall first use the corresponding functions of the Cloud Services. Where this is not possible through the Cloud Services, Analyste shall provide Customer with commercially reasonable assistance, without undue delay, taking into account the nature of the processing. Analyste shall further provide Customer with commercially reasonable assistance in ensuring compliance with Customer's obligations to perform security and data protection assessments, Security Incident notifications (see clause 4.8) and prior consultations of the competent supervisory authority, as set out in

the applicable data protection law, taking into account the nature of the processing and the information available to Analyste. Customer shall pay additional reasonable remuneration to Analyste for handling such assistance requests.

In case any individual or supervisory authority makes a request for assistance directly to Analyste concerning Personal Data, such as a request for access, rectification or erasure, delivering any information or executing any other action, Analyste shall inform Customer on such request as soon as reasonably possible and as far as allowed by applicable law.

4.3. **Location of Personal Data processing**. To provide the Cloud Services, Customer accepts that Analyste may have Personal Data processed and accessible by its Subprocessors (as defined in clause 6.1) outside Customer's country of domicile. However, Analyste warrants that no Personal Data is transferred from the European Economic Area ("EEA") to a Subprocessor.

4.4. **Data protection officer**. To the extent required by mandatory data protection law, Analyste appoints a Data Protection Officer, and shall communicate the relevant contact details to Customer upon request.

4.5. **Employees**. Analyste familiarizes its employees, authorized to process Personal Data, with relevant statutory data protection regulations, and ensures that these employees have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.6. **Technical and organizational security measures**. Analyste implements and maintains the appropriate technical and organizational security measures to protect Personal Data within its area of responsibility as detailed in annex 1 to this DPA. Analyste may modify its security measures from time to time but will not decrease the overall security during the term of the DPA.

4.7. **Security Incident notification**. In the event of any security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data processed by Analyste ("Security Incident"), Analyste shall, without undue delay after having become aware of it, notify Customer per applicable data protection law. Such notification shall allow Customer to perform any further notification as legally required. The Security Incident notification shall at least contain the following information:

a) description of the nature of the Security Incident, including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of Personal Data records concerned;
b) name and contact details of Analyste's contact point where more information can be obtained;
c) description of the likely consequences of the Security Incident; and
d) description of the measures taken by Analyste to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects.

In so far as it is however not possible to provide the information listed above at the same time, the information may be provided in phases without undue further delay. Analyste shall document any Security Incident, including the related facts, its effects and the remedial action taken. To the extent the Security Incident results from Analyste's breach of the Agreement, Analyste will use commercially reasonable efforts to remediate the cause of such Security Incident.

4.8. **Records of processing activities**. Analyste shall maintain a record of all categories of Personal Data processing that are subject to any EU member state's data protection law, carried out on behalf of Customer. This record contains the information as required by the Regulation and the applicable EU member state's data protection law.

5. AUDIT

5.1. **Documentation**. Analyste will have documented the activities taken to ensure compliance with its obligations under the Regulation, the applicable EU member state's data protection law and this DPA, at Analyste's cost.

5.2. **Audit.** To the extent further required, Customer may audit Analyste's compliance referred to in clause 5.1 according to the service level agreement.

5.3. **Costs**. Analyste will provide a copy of the documentation referred to in clause 5.1 and any existing documentation relevant to the audit referred to in clause 5.2, requested by Customer, free of charge. For any additional documentation, support or service requested by Customer, Analyste reserves the right to invoice the effort and arising reasonable cost to Customer. This shall also include adequate compensation for the working hours of Analyste staff while they are supporting Customer's audit, unless as far as the audit reveals that Analyste does not comply with its obligations under this DPA.

5.4. **Protection of Analyste's interests**. Where an audit may lead to the disclosure of business or trade secrets of Analyste or threaten intellectual property rights of Analyste, Customer shall employ an independent expert to carry out the audit, and the expert shall agree to be bound to secrecy to Analyste's benefit.

6. SUBPROCESSORS

6.1. **General authorization**. Customer gives its general authorization to allow Analyste to involve Analyste's affiliated companies and other subcontractors as subprocessors to process Personal Data in connection with the provision of the Cloud Services ("Subprocessors"), to the extent such appointment does not lead to non-compliance with any applicable law or Analyste's obligations under this DPA. Analyste ensures that the involved Subprocessors are properly qualified, will be under a data processing agreement with Analyste, and comply with data processing obligations similar to the ones which apply to Analyste under this DPA. Analyste regularly monitors the performance of its Subprocessors and is liable for their work towards Customer.

6.2. **Change of Subprocessor**. Analyste is free to choose and change Subprocessors. Upon request, Analyste shall inform Customer of the Subprocessors currently involved. In case there is a later change of Subprocessor (addition or replacement), Analyste shall notify Customer of such change. Should the processing be subject to any EU data protection law and should Customer demonstrate in writing that such new Subprocessor has breached any applicable data protection law and therefore not be able to support the involvement of that new Subprocessor, Analyste will undertake commercially reasonable efforts to remedy this situation. Should this not be remedied and Analyste continues to involve the related new Subprocessor for the Cloud Services, Customer shall be entitled to terminate the related part(s) of the Agreement for which the related new Subprocessor is involved, subject to three (3) months' prior notice, without any compensation or exit penalty being due by Analyste. To avoid any misunderstanding, should Customer not exercise this right of termination, it shall be deemed to support the involvement of the related Subprocessor and Analyste confirms to continue to be liable for this Subprocessor's work towards Customer, in accordance with clause 6.1.

7. TERM

7.1. **Term**. This DPA shall apply until the effective date of the termination of the Agreement. To the extent Personal Data is processed by Analyste after the effective date of termination of the Agreement, for whatsoever legitimate purpose, the terms of this DPA shall continue to apply to such processing for as long as such processing is carried out.

7.2. **Personal Data at the end of the DPA**. During a limited period of time from the date when the provision of the Cloud Services ends, Analyste shall make Customer Data (containing Personal Data) available to Customer as further specified in the Agreement. Within a reasonable time after expiry of the above mentioned limited period of time, Analyste shall permanently delete Customer's Personal Data from its storage media, except to the extent that Analyste is under a statutory obligation to continue storing such Personal Data. On Customer's request, Analyste shall confirm the deletion in writing. The obligation to delete Personal Data shall not apply to Personal Data

contained in regular backup copies of comprehensive datasets from which the individual deletion of Customer's Personal Data would not be possible without significant efforts or costs.

8. MISCELLANEOUS

8.1. **Customer Affiliates**. Both parties acknowledge and agree that, by signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable data protection laws, in the name and on behalf of its Affiliates that use the Cloud Services, if and to the extent Analyste processes Personal Data for which such Customer Affiliates qualify as data controllers as meant in clause 3.1. For the purposes of this DPA only, the term "Customer" includes Customer and its above meant Affiliates.

8.2. **Liability**. To the extent this DPA is concluded on behalf of Customer Affiliates as meant in clause 8.1, the liability cap specified in the Agreement shall, with regard to Analyste's liability under this DPA, be applied in aggregate, in a combined manner, to all claims together of Customer and concerned Customer Affiliates, related to the same event giving rise to liability, and shall not be understood to apply individually or severally to Customer and/or any of its concerned Affiliates.

8.3. **Indemnity**. Subject to the liability cap mentioned in the Agreement, Analyste shall indemnify Customer (subject to the specification in clause 8.2), and Customer shall indemnify Analyste for (i) administrative fines paid by the indemnified party and imposed on it by the competent supervisory authority, and (ii) damages paid by the indemnified party to natural persons based on a settlement (agreed by the indemnifying party) or final judgement, if the claim against the indemnified party results from breach of this DPA or any applicable data protection law by the indemnifying party, and only to the extent such breach is attributable to the indemnifying party. The indemnifying party shall provide, at its own cost, all reasonable support to the indemnified party in defending the claim. This clause 8.3 provides the indemnified party's exclusive remedy for all claims against it by any competent supervisory authority and natural persons.

8.4. **Compliance with laws**. Either party shall comply with the provisions of the data protection laws that specifically apply to its operations. More particularly, either party shall comply with the requirements of the Regulation and the applicable EU member state's data protection law implementing the Regulation, as of when they become enforceable, as far as they specifically apply to its operations. In the event any such statutory provision requires this DPA to be amended, upon request of either party, the necessary amendments shall be discussed in good faith, documented in writing and duly signed by both parties.

8.5. **Order of precedence**. This DPA is subject to the Agreement, to which it is added as Appendix.

9. ANNEXES

The below-listed annexes are incorporated into this DPA by this reference:

- Annex 1: Analyste Technical and Organizational Security Measures
- Annex 2: Personal Data in Analyste Products and Services

On behalf of **Customer** and, to the extent required under applicable data protection laws as specified in clause 8.1, in the name and on behalf of its **Affiliates** that use the Cloud Services:

Customer's signature of the Sales Agreement applies.

On behalf of **Analyste**:

Name:	Mr Mikko Soirola
Title:	CEO
Address:	Espoo, Finland

28.12.2018

Signature

December 28, 2018 Date of signature

28.12.2018

ANNEX 1: ANALYSTE TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Prevent unauthorized persons from gaining access to data processing sites that process and use Personal Data (site access control)

Personal Data is processed and stored in professionally hosted data centres, which are protected with effective physical access control, including electronic locks, burglar alarms and CCTV monitoring. Only nominated, authorized persons have physical access to data centre facilities. All visitors are accompanied at all times.

Prevent data processing systems from being used without authorization (system access control)

Each user of data processing systems is authenticated with a personal user account. Shared or group accounts are not used for personal access. Each user account must be approved by a management sponsor, and each user is personally responsible for the user account and the ways in which it is used. User accounts are reviewed regularly, and unnecessary users are removed.

Ensure that persons authorized to use a data processing system have access only to the data they are authorized to access (data access control)

Access rights to data processing systems are granted to pre-defined roles according to least privilege principle. Access to Personal Data must be justified with a clear and indisputable business need and approved by a management sponsor. Special admin, etc. privileges are granted to an absolute minimum number of users. Access rights are reviewed regularly, and unnecessary rights are removed.

Ensure that Personal Data cannot be read, copied, modified, or removed without authorization during electronic transfer, or when saving to data storage media (transfer control)

Electronic transfers of Personal Data in public networks are encrypted. Transfers within a data centre environment may not be encrypted; however, access to networks and processing systems is strictly limited by site and system access control. It is forbidden to store Personal Data to removable media. Backups of Personal Data are encrypted.

Ascertain and check where and to whom Personal Data can be transferred by means of data transmission facilities (disclosure control)

Transfer of Personal Data to non-production environments, such as testing, is forbidden without explicit customer approval or sufficient data masking.

Perform checks to establish whether and by whom Personal Data has been entered, modified, or removed in data processing system (input control)

Access to create, modify and remove Personal Data is logged, and an audit trail is created for all data processing systems. Audit trail logs are stored securely which prevents unauthorized modification or deletion of log events. Audit trail logs are stored in the service according to the service level agreement.

Ensure that Personal Data processed on behalf of a customer is processed in strict accordance with the service description and service level agreement (order control)

The scope of Personal Data protection is further described in the Personal Data Processing Appendix.

Ensure that Personal Data is protected against accidental destruction or loss (availability control)

Personal Data is backed up at regular intervals. Copies of data backups are transferred securely to an offsite location for disaster recovery. Data processing systems and infrastructure utilize redundant technologies, and single points of failure are minimized. Recovery time and point objectives are determined, and every effort is made to adhere to them.

Ensure that data collected for different purposes can be processed separately (separation control)

Personal Data is processed in dedicated systems that are not shared with other services, applications or corporate entities. Within individual systems and databases, data is segregated with logical access control. Personal Data will not be used for different purposes other than what it has been collected for without explicit customer approval.

Ensure that the customer is notified promptly in the event of a material breach of any of the controls above (notification control)

Customers will receive a prompt notification in the event of a Personal Data breach, a significant security incident in data processing system, or a material deviation from any of the controls above. In case Personal Data is lost or compromised, customer will be invited to participate in incident resolution, and can access applicable audit trail logs in the service.

28.12.2018

ANNEX 2: Personal Data in Analyste Products and Services

Annex 2 describes the storaging of personal data for the following products and services offered by Analyste Oy, later referred to as “the Service Provider”.

- Analyste Maksuliikenne for Windows
- Analyste Maksuliikenne for Windows SaaS
- Analyste Banking
- Analyste Banking SaaS
- Analyste Trezone SaaS

1. Personal data stored in the solutions

Personal data consists of the user management of the solutions. User management is an integrated part of the solutions and it is used to create personal user accounts for customer users who use the solutions. The intention of user management is to give access to authorized customer end-users to use the solution, according to the privileges and user rights that are granted to them by the customer organization.

- User login name
- User first name
- User family name
- User email address

2. Other data stored in the solutions

Other customer specific data stored in the solutions consists of customer organization specific data which is not considered as personal data. Such data is:

- Companies according to customer organization structure
    - Company name
    - Company registration number
- Banking information details of customer companies
    - Bank account number and currency
    - Name of bank and bank group
    - Cash pool name when applicable
    - Bank guarantee limit information when applicable
    - Bank guarantees issued by the customer companies
- Bank credentials for customer’s banks used by the customer organization to authenticate and log into the bank’s gateway services.
- Supplier and customer information as far as included in import data files, for example manual payments or guarantee issuance. Manual payments are individual payments that are entered into Banking manually and paid. Guarantee issuance can be utilized in the Trezone Guarantees module.

- Supplier or customer name
- Supplier bank account number for payments
- Supplier or customer contact address
- Supplier or customer contact phone number
- Supplier or customer contact email address

3. Access to personal data

Products and services offered and sold by the service provider can be categorized as Software-as-a-Service (SaaS) services where the service provider offers the solution from its own data center, or, as licensed software where the customer organization purchases the license to use the software and installs it in their own technical infrastructure.

3.1. Software as a Service (SaaS) provided by Analyste

Each user of the service is provided with an individual user account in the user administration of the service. Analyste provides the customer with one master user account in the beginning of the service implementation. The customer organization is responsible for creating and managing the necessary user accounts for their end users and managing their permissions.

Logging into the service requires a valid username and password. Personal data stored in the service can only be accessed by a valid user account that has the necessary user rights granted for user administration.

Analyste does not have access to the customer organization's service environment for the Maksuliikenne for Windows SaaS and the Banking SaaS services.

For the Analyste Trezone service, Analyste may use customer environment specific user credentials for service monitoring and health check purposes upon customer approval. The customer has the right to void the right without prior notice and their will.

Analyste may request the customer for temporary access to the customer organization's service environment for additional implementation work agreed together between the service provider and the customer, or in the case of incident solving. In both cases the customer organization's responsibility is to allow access to a named Analyste representative with adequate user rights required for the occasion. Once finished, it is the responsibility of the customer organization to disable access to the customer organization's service environment for Analyste representatives.

3.2. Onpremise license software sold by Analyste

Each user of the licensed software is provided with an individual user account in the user administration of the solution. Analyste provides the customer with one master user account in the beginning of the software implementation. The customer organization is responsible for creating and managing the necessary user accounts for their end users and managing their permissions.

Logging into the software requires a valid username and password. Personal data stored in the service can only be accessed by a valid user account that has the necessary user rights granted for user administration.

Analyste does not have access to the customer organization's software environment.

Analyste may request the customer for temporary access to the customer organization's software environment for additional implementation work agreed together between the service provider and the customer, or in the case of incident solving. Work is usually done in customer premises or by remote access specifically granted by the customer organization. In both cases the customer organization's responsibility is to allow access to a named Analyste representative with adequate user rights required for the occasion. Once finished, it is the responsibility of

the customer organization to disable access to the customer organization's software environment for Analyste representatives.

4. Location of personal data

Personal data is stored in the database of the solution. The data is encrypted.

For Software-as-a-Service (SaaS) provided by Analyste, the location of the data is within the European Union.

For licensed software installed by the customer organization in their own technical infrastructure, the location of the data is in the responsibility of the customer organization.

5. Storage time of data

5.1. Personal data

It is the responsibility of the customer organization to manage the personal data in the solution. Managing includes adding new data, editing existing data and deleting old data. For example, adding new data occurs when new user accounts are created or deleting old data occurs when user accounts are removed from the solution.

5.2. Other data

5.2.1. Banking SaaS

For Software-as-a-Service (SaaS) provided by Analyste, the storage time for business data in the Banking service is according to the Service Level Agreement, either two (2) or seven (7) years. The customer organization is responsible of downloading copies of the data to be stored locally in customer premises if so required. Business data stored in the service will be automatically deleted as the storage time expires.

5.2.2. Maksuliikenne for Windows SaaS

For Software-as-a-Service (SaaS) provided by Analyste, the storage time for business data in the Maksuliikenne service is according to the settings made by the customer organization. The storage time can be defined up to a maximum of 999 days. The customer organization is responsible of downloading copies of the data to be stored locally in customer premises if so required. Business data stored in the service will be automatically deleted as the storage time expires.

5.2.3. Trezone SaaS

For Software-as-a-Service (SaaS) provided by Analyste, the storage time for business data in the Trezone service varies based on the functional modules used.

- CashForecast module: 2 years
- Dealing module: service agreement period
- Guarantees module: service agreement period
- Netting module: service agreement period
- Reports module: service agreement period

The customer organization is responsible of removing data or downloading copies of the data to be stored locally in customer premises if so required. Business data stored in the service will be automatically deleted as the storage time expires or when the Service Agremeent terminates.

5.2.4. Onpremise license software

For onpremise license software sold by Analyste, the storage time for business data in the Maksuliikenne or Banking solutions is according to the settings made by the customer organization. The customer organization is

responsible of storing the data according to local requirements. Business data stored in the solution will be automatically deleted as the storage time expires.