Annex: Data Processing Agreement

Provisions on data protection and data security for commissioned data processing

concluded by and between

……..
……..
……..

– Controller –
(hereinafter referred to as “the Controller”)

and

INFORM Institut fuer Operations Research und Management GmbH
Pascalstrasse 35
52076 Aachen, Germany

– Processor –
(hereinafter referred to as “the Processor”)

(Both jointly hereinafter referred to as “Parties”)

Preamble

In order to specify the rights and obligations arising from the contractual data processing relationship in accordance with the statutory obligation under Art. 28 of the GDPR, the contracting Parties conclude the following agreement.

1 Subject matter, nature and purpose of processing

(1) In case of incidents the Processor support the Controller by analysing the case of incident. If the incident is caused by SyncroSupply software the Processor will deliver workarounds and bugfixes with the aim of maintaining the operational availability of the software system.

(2) Furthermore, the subject matter of the processing arises from the service agreement of SyncroSupply (as part of our SaaS contract) dated on …….…… (hereinafter referred to as “Main Agreement”), to which this refers to.

An additional processing of personal data of the Controller by the Processor is not intended.

(3) The processing of personal data takes place exclusively in the territory of the Federal Republic of Germany, in a Member State of the European Union, in another contracting state of the Agreement on the European Economic Area or in a state, that according to a Commission’s adequacy decision ensures an adequate level of protection. Any transfer to a third country requires the prior documented instruction of the Controller (Art. 28 para. 3 lit. a GDPR) and may only take place if the special requirements of Art. 44 - 49 GDPR are fulfilled.

2 Type of personal data, categories of data subjects

(1) Type of data:

- ☒ Personal master data (Name, Surname)
- ☒ Communications data (Telephone, E-mail, Preferred Language)
- ☐ Contract data (contractual relationship, product or contractual interests)
- ☒ Customer/client history
- ☐ Contract billing information and payment information
- ☒ Planning and control data (GPS-data)
- ☒ Information provided by third parties (Organisation, Qualification, Role)
- ☐ ……

(2) Categories of data subjects:

- ☒ Customers (business customer)
- ☐ Customers (consumer)
- ☐ Perspective Customers
- ☒ Employees
- ☒ Suppliers
- ☒ Service Providers
- ☐ ……..

3 Duration of the commission

(1) The duration of this commission ("Term") corresponds to the duration of the Main Agreement.

(2) Irrespective of the provisions of the Main Agreement, the Controller may terminate this Agreement at any time without notice if the Processor has committed a serious breach of the provisions of this Agreement, if the Processor cannot or does not wish to carry out instructions from the Controller, or if the Processor refuses to provide information or to grant the Controller access within the context of inspections, contrary to the contract. After termination, the Processor may no longer process any personal data of the Controller.

4 Responsibility and authority to issue instructions

(1) The Controller is responsible for compliance with data protection regulations, in particular for the lawfulness of data transfer to the Processor and for the lawfulness of data processing (Art. 4 no. 7 GDPR). The Processor shall not use the data for any other purpose and in particular shall not be entitled to pass them on to third parties. Copies and duplicates will not be made without the Controller's knowledge. Exceptions shall apply only to the extent specified in paragraph 2 of this clause.

(2) The Processor processes personal data only on documented instruction from the Controller, unless otherwise required under Union law or the law of the Member State to which the Processor is subject. In the event of any contrary obligation, the Processor shall immediately inform the Controller of the corresponding legal requirements before processing.

(3) If the Processor is of the opinion that an instruction infringes data protection regulations, the Processor shall inform the Controller without delay in accordance with Article 28 para. 3 sentence 3 GDPR. The Processor shall be entitled to suspend the execution of the instruction until such instruction has been confirmed or changed.

5 Confidentiality

The Processor shall only employ persons for the execution of the work who have committed themselves to confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b GDPR and who have previously been acquainted with the data protection provisions relevant to them. The Processor and any person under the Processor's control who has access to personal data may process such data exclusively in accordance with the instructions of the Controller, including the powers conferred in this Agreement, unless they are under a statutory obligation to process the data.

6 Data Security

(1) The Processor shall take appropriate technical and organisational measures for the appropriate protection of personal data, in accordance with Art. 28 para. 3 lit. c GDPR in conjunction with Art. 32 para. 1 GDPR, in order to guarantee the security of the processing by the Processor. For this purpose, the Processor shall

- ensure the confidentiality, integrity, availability and resilience of systems and services in connection with processing in the long term,
- ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident; and
- maintain a procedure for the regular review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the safety of processing.

The state of the art, the costs of implementation and the nature, scope and purpose of processing, as well as the risk of varying likelihood and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account.

(2) The contracting Parties agree on the data security measures laid down in **Annex 1 "Technical and organisational measures"** to this Agreement.

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. The safety level may not fall below the specified measures. Significant changes must be documented and communicated to the Controller in writing.

7 Engagement of other processors (subcontractors)

(1) For the purposes of this provision, subcontractors shall be processors commissioned by the Processor whose services relate directly to the provision of the main service. This does not include ancillary services used by the Processor, for example, telecommunication services, postal/transport services and cleaning.

However, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures to guarantee data protection and data security of the Controller's data, even in the case of outsourced ancillary services.

(2) The outsourcing to subcontractors or the change of the existing subcontractor is permitted, as far as:

- the Processor notifies the Controller in advance with a reasonable period of time in writing or in text form of such outsourcing to subcontractors, and
- the Controller does not raise an objection against the planned outsourcing in writing or in text form until the date of handover of the data to the Processor.

(3) A contractual agreement is to be concluded with the subcontractor in accordance with Art. 28 para. 3 and 4 GDPR, which meets the requirements for confidentiality, data protection and

data security of this Agreement. The Controller shall be entitled to inspect the Processor's contracts with subcontractors and to demand that the Processor send a copy of these contracts.

(4) The transfer of the Controller's personal data to the subcontractor and the subcontractor's first action shall only be permitted if all the prerequisites for subcontracting are met. The subcontractors approved by the Controller at the time of conclusion of the contract are listed in **Annex 2** to this contract.

(5) If the subcontractor provides the agreed service outside the EU/EEA, the Processor shall ensure the admissibility with regard to data protection law by means of appropriate measures.

(6) Further outsourcing by the subcontractor requires the express consent of the Processor (at least in text form). All contractual provisions in the contract chain must also be imposed on the other subcontractors.

8 Support in protecting the rights of data subjects

(1) The Processor is obliged to support the Controller with appropriate technical and organisational measures to protect the rights of the data subjects as specified in Art. 12 to 22 GDPR (Art. 28 para. 3 sentence 2 lit. e GDPR). In particular, the Processor shall support the Controller in fulfilling the claims of data subjects for deletion of their personal data in accordance with Article 17 GDPR.

(3) The Processor may only correct, delete or restrict the processing of personal data in accordance with documented instructions from the Controller (Section 11 para. 2 sentence 2 no. 4 and 10 BDSG / Art. 28 para. 3 sentence 2 lit. g GDPR). The Contractor may only provide information to third parties or the persons concerned after prior written consent by the Controller.

(4) If a data subject contacts the Processor directly in order to assert his rights in accordance with Articles 12 to 22 of the GDPR, the Processor will forward the request to the Controller without delay.

9 Support with documentation and reporting obligations

(1) If, according to Art. 37 GDPR, Section 38 BDSG-new, the Processor is legally obliged to appoint a data protection officer, the Processor shall inform the Controller of the data protection officer's contact details for the purpose of direct contact. A change of the data protection officer must be reported to the Controller immediately.

As data protection officer for the Processor,

Mrs. Astrid Ackermann, ics AG, Beim Strohhause 17, 20097 Hamburg

Email: aackermann@intersoft-consulting.ce

has been appointed.

(2) If the Processor becomes aware of a violation of the protection of personal data, he shall immediately notify the Controller of this violation pursuant to Art. 28 para. 3 lit. f, Art. 33 para. 2 GDPR. The same applies if persons employed by the contractor violate this Agreement.

(3) After consultation with the Controller, the Processor shall immediately take the necessary measures to secure the data and to minimise any possible adverse consequences for the data subjects.

(4) The Processor shall support the Controller with all information at his disposal in fulfilling the information obligations in relation to the competent supervisory authority in accordance with Art. 33 GDPR and, if applicable, in relation to the data subjects affected by the violation of the protection of personal data in accordance with Art. 34 GDPR.

(5) The Processor shall support the Controller with all information at his disposal in the data protection impact assessment pursuant to Art. 35 GDPR and, if necessary, in a prior consultation with the competent supervisory authority pursuant to Art. 36 GDPR.

(6) The Processor shall inform the Controller without delay of any checks and measures taken by the supervisory authority insofar as they relate to this Agreement.

10 Termination of the commission

(1) At the choice of the controller, the Processor deletes or returns all the personal data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(2) The Processor shall, without explicit request, prove to the Controller in text form with date indication that he has returned all data carriers and other documents to the Controller or that he has destroyed or deleted them in accordance with data protection regulations and has therefore not retained any of the Controller's data.

(3) The Processor shall keep any and all documentation which serves as evidence of the orderly and lawful data processing for the Controller beyond the end of the contract. The Processor can return them to the Controller at the end of the contract for his discharge.

11 Control rights of the Controller

(1) The Controller is entitled to regularly check the technical and organisational measures as well as compliance with this Agreement and data protection regulations before and during the provision of services relating to processing. For this purpose, the Controller or an authorized auditor may inspect the data processing equipment and the data processing systems of the Processor.

(2) For this purpose, the Processor shall be obliged to grant the Controller, during normal business hours, access to the premises where the Controller's data are physically or electronically processed. The Controller coordinates the inspections with the Processor in such a way that the operating procedures of the Processor are affected as little as possible.

(3) The Processor shall provide the Controller with all necessary information to prove the technical and organisational measures as well as compliance with this Agreement and data protection regulations. This information especially includes current attestations, reports or report extracts from independent bodies (e. g. financial auditors, external experts, IT security or data protection auditors) and suitable certification (e. g. according to the Basic Protection of the BSI – German Federal Office for Information Security). The contractor provides immediately the Controller with specific information on a case-by-case basis.

12 Liability

(1) Pursuant to Art. 82 para. 1 GDPR, the Controller and the Processor are liable in their external relationship for material and immaterial damage suffered by a person due to an

infringement of the GDPR. If both the Controller and the Processor are responsible for such damage in accordance with Art. 82 para. 2 GDPR, the Parties shall be liable internally for such damage in proportion to their share of responsibility. If, in such a case, a person asserts a claim for damages in whole or in part against one of the Parties, the other party may demand indemnification or indemnity from the other party to the extent that this is in proportion to their share of responsibility.

(2) The Processor is also liable to the Controller for compliance with data protection regulations by the subcontractors, which he uses to fulfil his tasks. The fault of subcontractors shall be attributed to the Processor as if it were his own fault.

(3) The Processor shall assist the Controller with all information at its disposal if the Controller is subject to administrative or criminal proceedings, to the liability of an affected person or a third party or to any other claim in connection with the processing of data with the Processor.

13 Final provisions

(1) Data carriers and data records provided to the Processor remain the property of the Controller.

(2) If individual or several clauses of this Agreement should be ineffective, the effectiveness of the remaining agreement is not affected. In the event that individual or several provisions of the contract are invalid, the Parties shall immediately replace the invalid provision with a provision which most closely resembles the invalid provision in terms of commercial interests and data protection.

(3) In the event of a contradiction between the Main Agreement and this Agreement, this Agreement shall take precedence in so far as the contradiction concerns the processing of personal data.

(5) The following Annexes form an integral part of this Agreement:

- Annex 1 „Technical and organisational measures“
- Annex 2 „Approved subcontractors“

Place, Date:	
Seal, Signature of the Controller	

Place, Date:	
Seal, Signature of the Processor	

Annex 1

Technical and organisational measures

Clause 6 of the Commissioned Data Processing Agreement refers to this annex for the specification of the technical and organisational measures.

Description of the technical and organizational measures as per Article 32 para. 1 GDPR

1 Confidentiality	**Confidentiality as part of information security** - suitable measures should ensure that information is only accessible to a defined set of users. *(e.g. locking, encryption, password rules, monitoring, certification)*

Entry control:

- Electronic access code cards / access transponders
- Authorised access process
- Video surveillance
- Alarm system
- Key management
- Visitors access accompanied by own employee
- Security outside of working times through plant security
- Graded security zones and controlled access
- Specially secured access to the data centre
- Servers stored in locked rooms
- Storage of the data carriers under lock and key or in locked rooms
- Storage of data backup (e.g. tapes, CDs) in access-protected safes

Admission control:

- Locking of data processing plants (e.g. locked cage for servers)
- Password protection of monitor workplaces
- Functional and/or time-limited granting of user privileges
- Use of individual passwords
- Automatic blocking of user accounts after multiple incorrect password entries
- Automatic password protected locking of the screen after a period of inactivity (screen saver)
- Password policy with minimum requirements on password complexity:
  - at least 8 characters
  - password change at least every 180 days
  - password history (no re-using of any of the last 10 passwords)
- hashing of saved passwords
  - SHA3
- Process of assignment of permissions on new entry of employees
- Process of withdrawing permissions when employees change department
- Process of withdrawing permissions when employees leave the company
- Required data secrecy in accordance with § 53 BDSG (new) (Federal Data Protection Act new)
- Controlled destruction of data carriers
- Storage of personal data in lockable security cabinets

Access control:

- Determination of access rights, permission concept
- Determination of authority to enter, alter, delete data
- Separation of permission authorisation (organisational) and permission granting (technical)

- Regulations on data recovery from backups (who, when, on whose request)
- Regular checking of permissions
- Limiting free and uncontrolled querying of data bases
- Regular evaluation of protocols (LogFiles)
- Partial access options to data inventories and functions (read, write, execute)
- Are corresponding security systems in place (software/hardware)?
- Virus scanners
- Firewalls
- Spam filters
- Limited access to LogFiles (only log admin)
- Saving of LogFiles on dedicated LogFile server

Separation control:

- File separation in data bases
- Logical data separation (e.g. on the basis of customer or client number)
- Processing of client and other customer data by different contractor employees
- Permissions concept meeting the need to carry out separate processing of client data from the data of other customers
- Functional separation
- Separation of development, test and productive systems

2 Contractor Control	**When personal data is processed "on behalf", it must be ensured that it is only processed in accordance with the instructions of the customer (see also section 1.5).**

- Drafting of contracts in accordance with legal requirements
- Central recording of existing service providers (uniform contract management)
- Prior checks at the contractor before the start of the contract
- Regular checks at the contractor after the start of the contract (for the duration of the contract)
- On-site inspections at the contractor's premises
- Review of the data security concept at the contractor's premises
- Inspection of existing IT security certificates of the contractors

3 Integrity	**Integrity as part of information security** - suitable measures should ensure that the correctness/integrity of data and correct functionality of systems is ensured. *(e.g. access limiting, checksums, fault analysis)*

Transfer control:

- What type of data sending exists between client and third parties?
  - VPN connection (IP-Sec)
  - Email with encrypted ZIP files
  - Data exchange via https connection
- Encryption protocol in use: TLS 1.2
- Encryption of confidential data carriers
- Encryption of laptop hard drives
- Encryption of mobile data carriers
- Data carrier disposal - secure wiping of data carriers:
  - Physical destruction (e.g. shredders for particle sizes to max. 1000 mm^2)
  - Paper disposal: secure destruction of paper documents
  - Locked metal containers (so-called data protection drums), disposal by service company
  - Shredders as per DIN 66399
- Packaging and sending prescriptions, encrypted email sending
- Direct collection, courier service, convoy
- Completeness and correctness monitoring

Input control:

- Reading, altering, deleting
- Partial access to data or functions
- Field access in data bases
- Obligation to data secrecy
- Regulation of data storage periods for audit/evidential purposes

4 Availability	**Availability as part of information security** - suitable measures should ensure that IT systems fulfil the requirements made of them in the time expected *(e.g. infrastructural measures, system maintenance, data security)*

Availability control:

- Data security and backup concepts
- Implementation of data security and backup concepts
- Limiting server room access to the necessary personnel only
- Fire alarm systems in server rooms
- Smoke alarms in server rooms
- Waterless fire-fighting systems in server rooms
- Climate-controlled server rooms
- Lightning/surge protection
- Water sensors in server rooms
- Server rooms in separate fire section
- Backup systems housed in separate rooms and fire sections
- Ensuring technical legibility of backup storage media for the future
- Storage of archive storage media in the required conditions (climate control, protection requirements, etc.)
- CO_2 fire extinguishers in direct proximity to server rooms
- Agreement regarding handover of (data) backups
- Storage of data in data security cabinets, vaults
- UPS (Uninterruptible Power Supply)

5 Resilience	**The resilience of the systems** should describe how they resist or are insensitive to software inadequacies, extreme numbers of requests, viruses, hacker attacks, etc. *(e.g. firewalls, virus scanners, intrusion detection systems, etc.)*

- Redundant power supply
- Redundant data connection
- Redundant air conditioning
- Redundant fire fighting
- Hard disc mirroring
- Deployment of a high availability SAN solution
- Load balancer
- Data storage on RAID systems (RAID 1 and higher)
- Delimitation of critical components
- Rapid and regular activation of available software and firmware updates
    - Identification of the various devices making up the network and determination of their hardware version and current software and firmware versions.
    - Communication channel with manufacturers to get informed about new updates and patches that are released for the devices owned.
    - Use of redundant systems to keep operations running while main devices are updated.
    - Progressive rollout of updates/patches to recognise problems early on without affecting several devices.

- Determination of a test period to check and ensure correct implementation of the update, so that operations can continue to run frictionlessly with the new updates.

- Security is included as a main concern during the design phase of the systems.
  - Limiting of permissions by need.
  - Revocation of temporary privileges as soon as they are no longer needed.
  - External customers and maintenance personnel receive specific access that is only active during their intervention and is deactivated the rest of the time.
  - Verification of new employees by background checks during commissioning and definition of exit interviews on leaving the organisation.
  - In the definition of network communication technologies and architecture, interoperability will also be included.
  - Identification of systems, infrastructures and environments that require intercommunication with other systems (internal or external) or will require this intercommunication in the near future (taking into account the life cycle or the involved devices).
  - Selection of communication protocols that are compatible with the identified systems and systems of the other organisations or environments.
  - Collaborative environments that allow the exchange of information between several parties.
- Periodic security training and awareness campaigns within the organisation.
  - Awareness campaigns to inform users about security concepts that are specific as much for concrete as for traditional IT systems.

6	**Processes to check all measures**	What documented regulations are there to make sure that the state of information security is regularly checked and updated? Is monitoring carried out, evaluated and the measures to be met checked up on?

- Internal process descriptions are updated at least yearly
- Notification of new/altered data processing procedures to the data protection officer
- Notification of new/altered data processing procedures to the IT security officer
- Data protection-friendly pre-settings are selected
- With negative results from previously mentioned monitoring, the security measures are adjusted, renewed and implemented on a risk-related basis

7	**Written documentation of:**
☒	Internal rules of conduct
☒	General data security description

Annex 2

Approved subcontractors

The Controller agrees to the commissioning of the following subcontractors, but only under the condition of a contractual agreement in accordance with Sections 11, 9 BDSG / Art. 28 para. 2-4 GDPR:

Company (subcontractor), address	Processing site	Type of service
AWS Amazon Web Services EMEA SARL 38 avenue John F. Kennedy L-1855 Luxemburg	AWS-Region EU-CENTRAL-1 Frankfurt, Germany	Data Processing Center