DATA PROCCESING AGREEMENT

Use of TrueLink services cf. Member terms (The main contract)

Concluded between

Member / Customer

Who is user of TrueLink services and have acceded **Member terms – TrueLink**, dated April 2018 or later

("Data Controller")

and

TrueLink A/S

CVR: 31261430

Havneparken 1, 1

7100 Vejle

("Data Processor", together "the parties" and individually "a party")

APPENDIX TO THE DATA PROCESSING AGREEMENT

Appendix 1 Instructions from the Data Controller
Appendix 2 Technical and organizational safety requirements and warranties
Appendix 3 The Data Controller's obligation
Appendix 4 Sub Data Processors
Appendix 5 Transfers to third countries and international organizations

1 BAGGROUND AND PURPOSE

1.1 The parties have agreed on delivering of services from the Data Processor to the Data Controller, as described in the data processor's member terms, of this ("main contract") described in appendix 1 to this agreement ("the Data Controller instruction")

1.2 In this regard, the Data Processor processes personal data on behalf of the Data Controller, for which reason the Parties have concluded this Agreement with underlying attachments ("The Data Processing Agreement")

1.3 The purpose of The Data Processing Agreement is to ensure that the Parties comply with the personal data regulation applicable at the Data Processing Agreement, i.e.:

(i) Personal data privacy act (law 2000-05-31 no. 429 with later changes)

(ii) General Data Protection Regulation (The European parliament and the council regulation (EU) 2016/679 on the 27th of April 2016), when this takes effect on the 25th of May 2018

2 EXTENT

2.1 The Data Processor is authorized to process personal data on behalf of the Data Controller under the terms set forth in the Data Processing Agreement.

2.2 The Data Processor may process personal data only by documented instruction from the Data Controller ("Instructions"). This Data Processing Agreement incl. Attachment is the Instructions at the Acceptance Date of the TrueLink Membership Terms.

2.3 The instructions may at any time be changed or further clarified by the Data Controller. Such changes are made in accordance with the change management process agreed between the Parties, cf. the Main Contract.

3 DURATION

3.1 The Data Processing Agreement is valid until the Main Contract expire.

4 DATA PROCESSOR OBLIGATIONS

4.1 Technical and organizational safety measures

4.1.1 The data processor is responsible for implementing the necessary (a) technical and (b) organizational security measures. The measures must be taken into account of the current technical level, implementation costs and the nature, extent, composition and purpose of the

treatment, and the risks of varying probability and seriousness of the rights and freedoms of the individuals, as well as the types of personal data described in appendix 1.

4.1.2 The Data Processor shall, notwithstanding paragraph 4.1.1, implement the technical and organizational security measures set out in appendix 2 to this Data Processing Agreement.

4.1.3 The Data Processor shall implement the appropriate technical and organizational measures in such a way that the Data Processor's processing of personal data complies with the requirements of applicable personal data regulation.

4.2 Terms of employees

4.2.1 The Data Processor shall ensure that employees who process personal data for the Data Processor have committed to confidentiality or are subject to appropriate statutory confidentiality.

4.3 Detection of compliance

4.3.1 The Data Processor shall, upon request, provide all information necessary to demonstrate compliance with the Data Processing Agreement requirements to the Data Controller and allow and contribute to audits, including inspections conducted by the Data Controller or other auditor who is authorized by the Data Controller. Such a request must be answered within a reasonable time.

4.3.2 For the purposes of Section 4.3.1, the Data Processor immediately informs the Data Controller if an instruction according to the Data Processor is contrary to data protection legislation or data protection provisions in other EU or national law.

4.4 List of treatment activities

4.4.1 Each Party shall keep records of treatment activities to the extent required by Article 30 of the Personal Data Regulation.

4.5 Security breach

4.5.1 The Data Processor shall inform the Data Controller without undue delay if the Data Processor becomes aware that there has been a violation of the personal data security.

4.5.2 The notification shall contain the facts of the breach of personal data security, its effects and the planned remedial measures.

4.6 Assistance

4.6.1 At the Data Controllers request, the Data Processor shall, as far as possible, assist the Data Controller through appropriate technical and organizational measures, with the obligation of the Data Controller to respond to requests for the exercise of the rights of the data subjects.

4.6.2 Considering the nature of the processing and the information available to the Data Processor, the Data Processor assists the Data Controller in ensuring compliance with the obligations of the Data Controller:

a) Security of processing,

b) Notification of breach of personal data protection to supervisory authorities,

c) Notification of breach of personal data protection to registered,

d) Impact Assessments on Data Protection, and Prior hearings.

5 THE DATA CONTROLLER'S OBLIGATIONS

5.1 The Data Controller has the obligations listed in appendix 5.

6 SUB DATA CONTROLLERS

6.1 The Data Processor may only use a third party for the processing of personal data for the Data Controller ("Sub-Processor") to the extent that it appears from (a) Appendix 4 to this Data Processing Agreement, or (b) Instructions from the Data Controller (Appendix 1).

6.2 The Data Processor and the Sub Data Processor must sign a written agreement which imposes on the Sub Data Processor the same data protection obligations as the Data Processor (including under this Data Processing Agreement).

6.3 In addition, the Sub Data Processor also deals with Instructors only from the Data Controller.

6.4 The Data Processor is directly responsible for the Sub Data Processor's processing of personal data in the same manner as was processed by the Data Processor himself.

7 TRANSFER TO THIRD COUNTRIES AND INTERNATIONAL ORGANIZATIONS

7.1 The data processor may only transfer personal data to a country outside the European Union or the EEA (a "Third Country") or international organizations to the extent that this is stated in (a) Appendix 5 to this Data Processing Agreement, or (b) Instructions from the Data Controller.

7.2 In any case, transfer of personal data may only occur if the Data Provider has secured a required transfer basis, for example the EU Commission Standard Contract Provisions.

8 DATA PROCESSING NOT ACCORDING TO INSTRUCTIONS

8.1 The Data Processor may process personal information outside the Instructions in cases where required by EU or national law to which the Data Processor is subject.

8.2 When processing personal information outside the Instructions, the Data Processor must notify the Data Controller of the reason for this. The notification must be made prior to the treatment and must contain a reference to the legal requirements underlying the treatment.

8.3 Notification shall not be made if notification will be in violation of EU law or national law.

9 REMUNERATION AND COSTS

9.1 The data processor is entitled to payment after due time as well as the Data Processor's other costs, for the services performed under the Data Processing Agreement at the Data Controller's request. The services may include, but are not limited to, changes to the instructions, assistance in reporting personal data breach, disclosure and deletion of information, audit assistance, expiration assistance, cooperation with supervisors, and assistance in compliance with requests from registered persons.

9.2 The Data Processor is entitled to payment after due time as well as the Data Processor's other costs, for the services performed under the Data Processing Agreement resulting from changes in the Data Controller. The services may include, but are not limited to, assistance for changes arising from new risk assessments and impact assessments as well as changes necessitated by changes in legislation.

10 OTHER PROVISIONS

10.1 General

10.2 Non-compliance

10.2.1 Non-compliance are governed by the TrueLink Membership Terms.

10.3 Responsibilities and Limitations of Liability

10.3.1 Responsibilities and Limitations of Liability are governed by the TrueLink Membership Terms.

10.4 Force Majeure

10.4.1 majeure is governed in TrueLink Membership Terms.

10.5 Confidentiality

10.5.1 Confidentiality is governed by the TrueLink Membership Terms.

11 TERMINATION

11.1 Resignation and termination

11.1.1 The Data Processing Agreement may be resigned or terminated only in accordance with the terms of resignation and resignation or termination in Membership Terms in relation to Appendix 1 Instructions from the Data Controller.

11.1.2 Resignation or termination of this Data Processing Agreement can only be done by - and entitled to - at the same time termination of parts of the agreement(s) regarding the provision of the Main Services relating to the processing of personal data under the Data Processing Agreement.

11.1.3 When the agreement(s) for delivery of the Main Services terminate, the Data Processor will continue to have effect until such personal data has been deleted or returned as described in Section 11.3.

11.2 Effect of termination

11.2.1 The regulation of the effect of termination is governed by the Main Contract.

11.3 The Data Processor and its Sub Data Processor shall return all personal data processed by the Data Processor under this Data Processing Agreement to the Data Controller at the Data Processing Agreement's end, to the extent that the Data Controller is not already in possession of the Personal Data. The data processor is then required to delete all personal data from the Data Controller unless otherwise stated in the Main Contract. The Data Controller may request the required documentation for this.

11.4 The Data Processor is entitled to anonymize personal information in such a way that they cannot be subsequently anonymized again, and then use the anonymous data for their own purposes both in the term of this Data Processing Agreement and forward.

12 DISPUTE RESOLUTION

12.1 The dispute resolution clause in the Main Contract shall also apply to this Data Processing Agreement as if this Data Processing Agreement was an integral part thereof.

13 PRECEDENCE

13.1 If there is any conflict between this Data Processing Agreement and the Agreement(s) regarding Delivery of the Main Services, this Data Processing Agreement shall prevail, unless otherwise provided directly by the Data Processing Agreement.

14 SIGNATURES

Vejle, April 1, 2019

The Data Controller	The Data Processor
Acceptance of TrueLink Membership terms logged in TrueLink Services.	Name: Per Hedeboe Jensen Title: CEO

APPENDIX 1
INSTRUCTIONS FROM THE DATA CONTROLLER

15 PURPOSE AND MAIN CONTRACT

15.1 The main contract is meant: TrueLink Member terms.

16 PERSONAL DATA

16.1 Types of personal data, processed in connection to delivery of the main benefit:

a) General personal data

b) Sensitive personal data, including health information (if applicable)

c) Social security number (if applicable)

16.2 The category of registered identified or identifiable natural persons covered by the Data Processing Agreement:

a) Username, first name, last name, e-mail and telephone number.
b) Creation of own customers, with information about name, address, telephone and e-mail address
c) Creation of own suppliers with name, address, telephone and e-mail address
d) Document data with information about sender / recipient of personal data, as well as content in the document in the form of Beneficiary, Social security number.
e) It is the Data Controller's responsibility that personal data is placed correctly in the documents

TrueLink A / S will limit access to data in the TrueLink service in connection with the imposition of the Personal Data Regulation on May 25, 2018:

- Invoice form and credit note display form, where a CPR number appears in the content of the display form, this content will be marked with xxxxxx-xxxx
- Access to 3-level log where it is possible to view / download raw data, such as XML, CSV, etc., where personally sensitive data can be seen
- Administrator can modify this restriction on the Customer's account in TrueLink for all users with access to the Customer's account. Such a change will be logged in the TrueLink personal data log.

APPENDIX 2
TECHNICAL AND ORGANIZATIONAL SAFETY

General safety precautions

TrueLink has developed and implemented information policies based on ISO 27001: 2013 and ISO 27002: 2017 standards. In the following are sections of TrueLink's information security policies copied. In accordance to TrueLink's information security policies review shall happen at least once a year to ensure that changes in the threat assessment are taken into account, along with changes to TrueLink, etc. TrueLink sets its information security policies for review for customers and collaborators.
For reference to TrueLink's internal documentation of information security policies, we have the following options to use the same paragraph numbers as in the internal documentation

Authorization and access control
Access Control
9.1 Business requirements for access control
TrueLink systems are protected by authorization systems designed to protect against unauthorized access. TrueLink users assist in protecting information assets through proper use of authorization systems.

9.1.1 Access Control Policy
Only access to relevant information
User authorization for systems and systems data is limited, leaving access to systems and data only to the extent that users have a work-related need for access.

9.1.2 Access to networks and network services
Division of networks
TrueLink's network is divided into corporate networks and guest networks. Only TrueLink employees and external consultants have access to the corporate network and guests can access guest networks.

Connection to hosting - other outsourcing partners
All connections between TrueLink's offices, hosting centers, outsourcing partners and customers are established through secure VPN connections or certificate connections, and where connections only provide access to necessary service.

9.2 User Access Administration
TrueLink has a fixed procedure for starting, changing, and terminating collaborative relationships, which prescribes updating documentation for assigned rights to users on TrueLink systems. The procedure and the listing include common user access and rights as well as the grant of privileged user rights as well as user access to privileged system programs.

It is the system owner who gives user access and rights, in particular "09.02 Procedure for Starting, Changing, and Terminating Collaborative Relationships" as well as ensuring that "09 List of Users and Rights" is updated by changes.

9.2.1 User registration and registration
Identification, authentication and authorization of users
All users are assigned a unique identity in TrueLink systems, which are for personal use only. Appropriate authentication technology has been set up to verify user identity. To have full traceability of a user's activities on TrueLink's systems, it is not permitted to use common user identities on TrueLink systems.
Cancellation of user upon termination of cooperation
In connection with the termination of collaboration where users must be discontinued in TrueLink's systems, TrueLink has a fixed procedure for abandoning users.

Reference: "09.02 Procedure for Start, Change, and Termination of Collaboration" and Documentation of "09 List of Users and Rights".

9.2.2 User Access Assignment
In connection with start-up and change of relationship, TrueLink has a procedure for granting / removing rights, the procedure also prescribes user and rights registry updating.

User rights must match the business needs, which must be checked after a user has been created.
Reference: "09.02 Procedure for Start, Change, and Termination of Collaboration" and Documentation of "09 List of Users and Rights".

9.2.3 Control of privileged access rights
Privileged / Administrator Access Rights
Allotment of privileged access privileges, granted only when there is a business need and only granted by prior approval from TrueLink's management, TrueLink has a fixed procedure for granting access to privileged access privileges.

Reference: "09.02 Procedure for Start, Change, and Termination of Collaboration" and Documentation of "09 List of Users and Rights".

Privileged system programs
Allotment of access to privileged system programs is only granted when there is a business need and only granted by prior approval from TrueLink's management. TrueLink has a fixed procedure for granting access to privileged system programs.

Reference: "09.02 Procedure for Start, Change, and Termination of Collaboration" and Documentation of "09 List of Users and Rights".

Change system administrator passwords
System administrator passwords must be changed after a maximum of 60 days. System Administrator passwords must be changed if there is the slightest suspicion that outsiders are aware of the password and it should also be changed immediately after collision termination with a user / person who is aware of system administrator passwords.

General system administrator user profiles that can be used on TrueLink systems are only used in emergency situations and therefore never in the daily work of TrueLink.

Reference: "09.02.03 Procedure and Log Change of Administrator and System Passwords" and "09 Administrator and System Passwords List"

9.2.4 Management of secret authentication information about users

Requirements for password

Users must change their password after a maximum of 90 days, password must be of a minimum length of 8, contain numbers, uppercase and lowercase.

Password Guidelines

When creating users, these must be assigned a secure temporary password to be changed at first login.

Password storage

Passwords must not be stored in clear text, either in digital form or on paper.

Administrator password, stored electronically in documents that are password protected and the password is only known by TrueLink's management.
Reference: "09 List of Administrator and System Passwords"

Transfer of password

A password can never be transferred or shared with others, the only exception is when a user must log in for the first time with temporary password where system owners can assign the temporary password to the user.

9.2.5 Review of user access rights

Internal audit of user profiles and rights

The procedure for reviewing user profiles and rights in TrueLink's systems is described, the procedure prescribes that all user profiles and user groups are reviewed to ensure that no inactive users or user groups exist. In addition, all users 'rights must be verified including privileged rights as well as access to privileged system programs to ensure that the allocation of rights is in line with users' business needs.

Reference: "09.02.05 Procedure and log on internal audit of users and rights".

9.2.6 removal or adjustment of access rights

Removal of access rights

Upon termination of a relationship, the user must be deactivated as a minimum to prevent access to TrueLink systems. After a maximum of 30 days, the user must physically erase from TrueLink's systems.

Access Rights Adjustment

When changing a cooperative relationship, access rights must be reviewed so that the rights reflect business needs.

Reference: "09.02 Procedure for Start, Change, and Termination of Collaboration" and Documentation of "09 List of Users and Rights".

9.3 User responsibility
9.3.1 Use of secret authentication information
Use of one's password
It is allowed to use the same password in TrueLink systems, it is not permitted to use the same TrueLink password on the Internet that is used on the TrueLink system (s), for example. by access to Facebook, private banking etc. Large password reuse increases the risk that password confidentiality may be violated,

Content in password
It is the user's responsibility to make password as secure as possible, i.e. avoid birthdays, names of friends / family / pets, etc.

Password tags for TrueLink systems must be at least 8 characters and must be a combination of the following:
• Uppercase
• Lowercase
• Numbers

Change password
Passwords must be changed at least after 90 days.

”Auto Login”
It is not permitted to use systems where passwords are stored in shortcuts, function keys, macros or the like. form of auto save mode.

Password storage
The user's password must never be in plain text on any media, such as. paper, in Word document, in Notepad document or similar.

9.4 Control of system and application access
9.4.1 Limited access to information
TrueLink systems only allow access to information to the extent that the user has rights to this. I.e. Access to data classified as confidential or higher is restricted to the widest extent possible.

9.4.2 Safe Log-On Procedures
Access to TrueLink's systems is protected by secure log-on procedure, where usernames are used to identify the person who logs in. The person is responsible for the activities performed by the person on the system for that log-on.

9.4.4 Use of privileged system programs
The use of privileged system programs is limited to the maximum extent and is granted only when it is business-relevant to provide access. Rights are awarded in the procedure for starting, changing and terminating cooperative relationships.

Reference: "09.02 Procedure for Start, Change, and Termination of Collaboration" and Documentation of "09 List of Users and Rights".

9.4.5 Control of access to source codes for programs

Developer and user access to source code is restricted by allowing access only to the source code of the systems being developed. Rights are awarded in the procedure for starting, changing and terminating cooperative relationships

Reference: "09.02 Procedure for Start, Change, and Termination of Collaboration" and Documentation of "09 List of Users and Rights".

Input material containing personal information

4 Guidelines for storing and deleting data
TrueLink systems are made available to customers where customers have input material that is updated in TrueLink's systems.

Storage of output and input occurs in TrueLink systems until customers give instructions to delete and / or output, or parts thereof.

This means that TrueLink's guideline is that input and output are stored until the data manager gives instructions to delete in input and / or output

All data is protected for this purpose. TrueLink’s Information Policies.

Output material containing personal information

4 Guidelines for storing and deleting data
TrueLink systems are made available to customers where customers have input material that is updated in TrueLink's systems.

Storage of output and input occurs in TrueLink systems until customers give instructions to delete and / or output, or parts thereof.

This means that TrueLink's guideline is that data and output are stored until the data manager gives instructions to delete in input and / or output

All data is protected for this purpose. TrueLink’s Information Policies.

External communication connections

10.1.1 Policy for the use of cryptography.
Communication links
TrueLink's connections to collaborators are always conducted on secure lines, either as VPN tunnels, HTTPS communications, and private / public key, to protect confidential / secret / very secret information that is being transmitted between TrueLink and collaborators.

10.1.2 Key management
A key management system has been established that contains information about all established keys and between which partners / points.

Check with rejected access attempts

9.4.3 Password management system
With more than 3 consecutive attempts at login, the TrueLink systems shut the user out until the system owner closes the user again.

If a user is shut out, without the user being responsible for this, the event must be logged in to TrueLink event log. Reference to: "16 TrueLink Event Management Procedure".

Logging

12.4 Logging and surveillance
12.4.1 Incident logging
Incident logging takes place in "Registered incident" where TrueLink logs incidents that are observed or reported from, for example, outsourcing partners, customers, etc.

Reference to: "16 TrueLink Event Management Procedure"

Application logging / logging of user activity
TrueLink systems log in the application log when users perform viewing, creation, modification or deletion of data.

Log history is stored until TrueLink's customers, instructs that log history be deleted.

12.4.2 Administrator and Operator Log
Logging of all actions performed by users with administrator privileges in connection with system components, DB, server administration, etc., is logged.

Home office
The supplier's processing of personal data is done in whole or in part by the use of workplaces at home.

6.2 Mobile equipment and remote Jobs
6.2.2 Remote Jobs
Only TrueLink-owned PCs must be connected to TrueLink via VPN.
Printing confidential / secret / very secret information on printers outside of TrueLink's domain should be avoided as far as possible. In situations where it is necessary, the prints must be kept safe until shredding can be done at the TrueLink office.

APPENDIX 3
THE DATA CONTROLLER'S OBLIGATIONS

1 OBLIGATIONS

1.1 The Data Controller have the following obligations:

1.1.1 The Data Controller is responsible for complying with the personal data privacy act currently in force in relation to the personal data that is left to the Data Processor's processing. The Data Controller is, in particular, responsible for and insists that:

- The statement in Appendix 1 is exhaustive and the Data Processor can act accordingly, including: in relation to the determination of necessary safeguards.
- The Data Controller has the necessary authority to process and to leave it to the Data Processor to process the personal data processed in connection with the provision of the Main Services.
- The instructions given, according to which the Data Processor must process personal data on behalf of the Data Manager, is legal.

1.1.2 The Data Controller briefly informs the Data Processor of possible impact assessments that are relevant to the discontinued processing activities, and the Data Controller, at the same time, provides the Data Processor with insight into the analysis in order for the Data Processor to fulfil his obligations under the Data Processing Agreement.

1.1.3 The Data Controller also informs the Data Processor of matters of significance to the Data Processor performing its obligations under the Data Processing Agreement, including, among others, the Data Controller continuous risk assessment, to the extent that they are relevant to the Data Processor.

1.1.4 The Data Manager also informs the Data Processor if the personal data security act currently in force in relation to the personal data that is left to the Data Processor's processing includes other than Law No. 429 of 31/05/2000, with subsequent changes in the processing of personal data (personal data security act) or Regulation of the European Parliament and the Council (EU) 2016/679 (including subsequent adaptations of Danish law resulting from this Regulation).

1.1.5 The Data Controller assists the Data Processor to enter into agreements with Sub Data Processors to the necessary extent, including to ensure transfer to third countries.

APPENDIX 4
SUB DATA PROCESSORS

1 GENERAL

1.1 The Data Controller hereby gives its prior general approval to the Data Processor to make use of a Sub Data Processor. The Data Processor shall notify the Data Controller in writing of the addition or replacement of a Sub Data Controller prior to the commencement of the application. Similarly, the Data Processor shall notify the Data Controller of termination of use of a Sub Data Processor.

1.2 The Data Processor use the following Sub Data Processor:

1) Itadel A/S (CVR number: 37032034)
   Operation of TrueLink A/S' solutions
   Address: Sletvej 30, 8310 Tranbjerg J

2) TrueDevelop Sp. Z o. o., PL (KRS number 0000754117, NIP 5272868353)
   Development and last level support for TrueLink A/S' solution
   Ul. Mazowiecka 11 app. 49,00-052 Warszawa, Poland

3) Interoperability partner
   a) TrueCommerce ApS (VANS/EDIFACT sending and receiving)
   b) mySupply A/S (sending to Norway and other PEPPOL countries)
   c) Inexchange AB (sending and receiving from Sweden and Finland)
   d) Pagero AB (sending and receiving from Sweden and Finland)
   e) Basware AB (sending and receiving from Sweden and Finland)
   f) Crediflow AB (sending and receiving from Sweden and Finland)

APPENDIX 5
TRANSFER TO THIRD COUNTRIES AND INTERNATIONAL ORGANIZATIONS

1 GENERAL

1.1 Through its acceptance of the TrueLink Membership, the Data Controller hereby authorizes the Data Processor to enter into EU Standard Contract Provisions for Transfer of Personal Data to a Third Country or International Organization on behalf of the Data Controller with the Sub supplier.

1.2

Company	Country or location
Microsoft Valid Transfer Warranty: EU-U.S. Privacy Shield	USA