Data Processing Agreement
for

Jungheinrich Digital Products and Software Solutions

(hereinafter: "**Agreement**")

Between

the costumer designated in the FMS main Contract (One-time Contract)

- hereinafter referred to as "**Customer**" -

and

JUNGHEINRICH Hungária Fejlesztési és Tanácsadó Korlátolt Felelősségű Társaság

Seat: 2051 Biatorbágy Vendel Park, Tormásrét u 14.
RegNo: 13-09-070761

- hereinafter referred to as "**Jungheinrich**" -

- hereinafter also referred to as the Customer and Jungheinrich are also each individually referred to as a "**Party**", and jointly as the "**Parties**" -

PREAMBLE

A. A contract or several contracts exist between the Parties for the provision of certain Digital Products and Software Solutions from Jungheinrich or the performance of Maintenance and Support Services by Jungheinrich for the Customer (collectively the "**Main Contract**"). As part of the provision of the services agreed under the Main Contract, Jungheinrich shall also process Personal Data on behalf of the Customer to the extent described in **Appendix 2** to this Agreement.

B. The Parties agree that the following provisions shall apply to the Processing of Personal Data by Jungheinrich on behalf of the Customer when providing the contractual services.

1. DEFINITIONS

In the context of this Agreement the following terms have the following respective meanings:

1.1 "**Affiliate**" for the purposes of this Agreement means any other company in relation to one of the Parties which directly or indirectly controls the respective Party, is controlled by it or is under common control with it. For the purposes of this definition, "control" means direct or indirect ownership or ownership of more than fifty percent (50%) of the voting interest in an entity; the terms "controlling," "controlled by," or "under common control" shall have the meanings corresponding to the foregoing.

1.2 "**Applicable Data Protection Law**" means the laws, rules and regulations referred to in Clause 2.3.

1.3 "**Appropriate Expense-Related Remuneration**" means remuneration of Jungheinrich by the Customer based on the actual time spent and on the basis of the hourly rates agreed between the Parties in the Main Contract, including reimbursement of any material expenses incurred by Jungheinrich (Time & Material). In the event that the Parties have not agreed on hourly rates either in the Main Contract or within the framework of this Agreement, the hourly rates customary in the market shall be deemed to have been agreed for the respective activity.

1.4 "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. The Customer is the Controller for the Processing of Personal Data by Jungheinrich on behalf of the Customer to the extent regulated in this Agreement.

1.5 "**Customer**" means the company referred to in the preamble and its Affiliates that have been included in this Agreement in accordance with Clause 3.1 .

1.6 "**Data Subject**" means the person to whom Personal Data refers.

1.7 "**EU Data Act**" means Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules for fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

1.8 "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.9 "**Involved Affiliate**" means an Affiliate (i) in whose name and on whose behalf the Party that is affiliated with the company has entered into this Agreement (Clause 3.1), or (ii) that has subsequently acceded to this Agreement in accordance with Clause 3.2.

1.10 "**Jungheinrich**" means the company so designated in the preamble and its Affiliates that have been included in this Agreement pursuant to Clause 3.1

1.11 "**Personal Data**" is any information relating to an identified or identifiable natural person.

1.12 "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.13 "**Processor**" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller. Jungheinrich is a Processor in the scope of its Processing of Personal Data on behalf of the Customer to the extent regulated in this Agreement.

1.14 "**Sub-processor**" means an additional Processor or Processors within the meaning of Art. 28 para. 2, 4 GDPR.

2. SUBJECT-MATTER, PURPOSE AND TERM OF THE AGREEMENT; APPLICABLE LAW

2.1 Subject-matter and purpose of the Agreement

The subject-matter of this Agreement is the Processing of Personal Data by Jungheinrich (as a Processor) on behalf of the Customer (as a Controller) in the context of the provision of the services agreed under the Main Contract to the extent described in **Appendix 2**. Data Processing operations under Jungheinrich's own responsibility, as described in Clause 4.3, among others, remain unaffected by this Agreement.

This Agreement serves to comply with the provisions of Art. 28 (3) and (4) GDPR. It does not serve to regulate the details of the provision or use of product data and associated service data within the meaning of the EU Data Act.

2.2 Term of the Agreement; cancellation

The term of this Agreement shall be the term of the Main Contract. If the Main Contract consists of several components with different terms, the term of this Agreement begins with the start of the term of the Main Contract component that begins first and ends with the term of the Main Contract component that ends last.

The rules on termination in the Main Contract and in 11.3 of this Agreement apply.

2.3 **Applicable law**

The provisions of the GDPR, the relevant national regulations for the implementation and introduction of the GDPR, all other data protection laws at the registered office of the Parties and the legally binding data protection decisions of the competent courts (collectively "**Applicable Data Protection Law**") shall apply to the data protection provisions of this Agreement and their interpretation.

The law at the registered office of Jungheinrich applies to all non-data protection regulations.

3. PARTIES TO THE AGREEMENT

3.1 **Involvement of Affiliates**

The Parties conclude this Agreement in their own name as well as in the name and on behalf of their Affiliates, insofar as this is desired by the respective Party and a corresponding power of attorney exists. The Parties are obliged to document the existence of a proper power of attorney and to provide evidence of this in a suitable form at the request of the other Party. In order to document the Involved Affiliates that are party to this Agreement, the Parties shall exchange a list of the Involved Affiliates and update it as required.

Each Affiliate of the Customer involved in this way is hereby bound to comply with the requirements of this Agreement and shall have the rights and obligations of a Controller under this Agreement. Each Jungheinrich company involved in this way is hereby bound to comply with the provisions of this Agreement and has the rights and obligations of a Processor under this Agreement.

The Involved Affiliates do not automatically become a party to the Main Contract as a result of the provision in this Clause 3.1, but only a party to this Agreement.

3.2 **Subsequent accession**

An Affiliate of one of the Parties that is not a party to this Agreement at the time the Agreement is concluded may join this Agreement at any time on the part of the Party affiliated with such Affiliate by signing a declaration of accession in accordance with the model in **Appendix 1** and sending it to the other Party. In the event that the other Party does not object to the accession in writing or text form within two (2) weeks, the acceding Affiliate shall become a party to this Agreement and shall henceforth have the rights and obligations of a Controller or Processor under this Agreement. No rights or obligations resulting from this Agreement shall apply to the acceding Affiliate for the period prior to its accession as a party.

3.3 **Collective exercise of rights**

Unless the assertion of any right or remedy under this Agreement by the Involved Affiliate on the part of the Customer itself is required by law or expressly agreed otherwise by the Parties, the exercise of the rights under this Agreement available to the Involved Affiliates on the part of the Customer under Applicable Data Protection Law

i. may only be exercised by the Customer, who is a Party to the Main Contract, on behalf of the Involved Affiliates on the part of the Customer, and

ii. in each case only in an aggregate manner, that is, not individually for each Involved Affiliate, but collectively for itself and all Involved Affiliates together.

This collective exercise of rights also relates to the exercise of the control rights in accordance with Clause **Hiba! A hivatkozási forrás nem található.**. In this context, the Customer, who is a Party to the Main Contract, shall ensure that any interference with Jungheinrich's operations in the event of any on-site inspections is kept to a minimum by bundling and combining inspection requests from several Involved Affiliates for an on-site inspection as far as possible.

4. SPECIFICATION OF THE CONTENT OF THE AGREEMENT

4.1 **Details of data Processing on the Customer's behalf**

The Processing of Personal Data by Jungheinrich on behalf of the Customer is carried out to the extent necessary for the provision of the services agreed under the Main Contract. The scope therefore depends on which Jungheinrich Digital Products and Software Solutions Jungheinrich's services relate to. The details of data Processing by Jungheinrich on behalf of the Customer, in particular the categories of Personal Data, the categories of Data Subjects and the purposes for which the Personal Data is processed on behalf of the Customer, as well as the regular retention period, are listed in **Appendix 2**.

4.2 **Place of Processing on behalf**

The provision of the contractually agreed data Processing on behalf of the Customer shall take place in a member state of the European Union (EU) or in another state party to the Agreement on the European Economic Area (EEA), unless otherwise stipulated in this Agreement.

Any transfer of data by Jungheinrich to recipients in a country outside the EU or the EEA ("**Third Country**") or an international organisation shall be made solely on the basis of documented instructions from the Customer or to comply with a specific provision under Union law or the law of an EU Member State to which Jungheinrich is subject and must comply with Chapter V of the GDPR or Regulation (EU) 2018/1725.

The Customer agrees that in cases where Jungheinrich engages a Sub-processor pursuant to Clause 11 to carry out certain Processing activities (on behalf of the Customer) and where the Processing activity involves a transfer of Personal Data to a Third Country within the meaning of Chapter V of the GDPR, the Processing may take place in a Third Country outside the EU/EEA if

- there is a decision by the EU Commission that an adequate level of protection is ensured in this Third Country, or
- Jungheinrich and the Sub-processor use standard contractual clauses issued by the European Commission pursuant to Art. 46 (2) of the GDPR, or
- another recognised transfer mechanism within the meaning of Chapter V of the GDPR is used.

In the event that the Customer has its registered office in a Third Country, the Parties shall, to the extent necessary, enter into a separate Agreement that ensures compliance with the data protection law applicable at the Customer's registered office.

4.3 **Processing of data for Jungheinrich's own purposes**

In the event that Jungheinrich processes Personal Data (in the sense of personal identifiable machine data such as equipment ID, timestamp, etc.) or non-Personal Data regarding the Customer's use of the Digital Jungheinrich Products, applications, tools, platforms, software, hardware and/or additional services for Jungheinrich's own purposes, Jungheinrich is the Controller regarding this Processing in accordance with the applicable general terms and conditions of Jungheinrich that form part of the Main Contract. This Agreement does not apply to such data Processing for Jungheinrich's own purposes.

5. TECHNICAL AND ORGANISATIONAL MEASURES

5.1 Jungheinrich shall apply the technical and organisational measures listed in **Appendix 3** in accordance with the Customer's instructions in order to ensure a level of protection appropriate to the risk of data Processing with regard to the confidentiality, integrity and availability of the Customer's Personal Data processed on behalf of the Customer as well as sufficient resilience and security of the systems used for data Processing. In doing so, Jungheinrich will take into account the state of the art, the implementation costs and the nature, scope and purposes of the Processing as well as the varying

likelihood and severity of the risk to the rights and freedoms of natural persons.

The technical and organisational measures are subject to technical progress and further development. In this respect, Jungheinrich is permitted to implement alternative adequate measures as long as the security level of the defined measures is not undercut. Jungheinrich will document significant changes by adapting**Appendix 3** .

5.2 Insofar as an audit by the competent supervisory authorities reveals a need for adjustment with regard to the technical and organisational measures applied, the Parties shall implement this by mutual Agreement within a reasonable period of time and Jungheinrich shall adapt **Appendix 3** accordingly.

6. CUSTOMER'S AUTHORITY TO ISSUE INSTRUCTIONS

6.1 Within the scope of this Agreement, Jungheinrich shall Process Personal Data exclusively within the framework of the agreements made and in accordance with the Customer's instructions, unless it is obliged to Process such data in accordance with the law of the EU or the EU/ EEA member states to which it is subject; in such a case, Jungheinrich will notify the Customer of these legal requirements prior to Processing, unless the law in question prohibits such notification due to an important public interest. The instructions are initially defined by this Agreement and may thereafter be amended, supplemented or replaced by the Customer by means of individual instructions in writing or in an electronic format (text form) to the office designated by Jungheinrich (individual instruction). All instructions given shall be documented by both Parties and kept for the duration of the cooperation.

6.2 The Customer shall confirm verbal instructions in writing or electronically.

6.3 Jungheinrich shall not use the Personal Data processed on behalf of the Customer for any purposes other than those agreed, in particular not for its own purposes or the purposes of third parties. Copies and duplicates shall not be made without the Customer's knowledge. Excluded from sentences 1 and 2 are backup copies insofar as they are necessary to ensure proper Processing, the cases of use for own purposes in accordance with Clause 4.3 and the Processing of Personal Data that is necessary with regard to compliance with statutory retention obligations.

6.4 Jungheinrich shall immediately inform the Customer, if Jungheinrich is of the opinion that an instruction violates data protection regulations. Jungheinrich shall be entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by a responsible person on the part of the Customer.

6.5 The Customer warrants that the instructions issued to Jungheinrich for the Processing of Personal Data comply with applicable law. The Customer shall indemnify Jungheinrich against any third-party claims arising from non-compliance with this warranty.

6.6 The Customer and Jungheinrich shall each designate to the other Party those persons (and any changes of such designated persons) who are authorised to issue instructions or receive instructions in accordance with this Agreement. The designation shall be made in text form or writing and in each case via the usual means of communication between the Parties. If the Parties have not agreed any other means of communication, designation by e-mail is permissible and sufficient.

6.7 Insofar as an instruction goes beyond the services agreed in the Main Contract, Jungheinrich may demand Appropriate Expense-Related Remuneration for its fulfilment.

6.8 Insofar as Jungheinrich processes Personal Data under its own responsibility (see Clause 4.3), Jungheinrich is not bound by the Customer's instructions.

7. SUPPORT OF THE CUSTOMER IN THE EVENT OF THE ASSERTION OF DATA SUBJECT RIGHTS

7.1 If a Data Subject raises a statutory claim directly against Jungheinrich for information, rectification, erasure, restriction of Processing, data portability, objection and the omission of a decision based solely on an automated decision (collectively: "**Data Subject Rights**") with regard to his or her Personal Data processed by Jungheinrich on behalf of the Customer, Jungheinrich shall forward this request to the Customer without undue delay. Jungheinrich shall only rectify, erase or restrict the Processing of the Personal Data of the Data Subject making the claim, provide information to the Data Subject making the claim or fulfil the Data Subject's right to data portability upon documented instruction from the Customer. This reservation of prior instruction by the Customer does not apply to any data Processing by Jungheinrich due to official or court orders in connection with the rights of the Data Subject.

7.2 The Customer shall pay Jungheinrich an Appropriate Expense-Related Remuneration for its support of the Customer in safeguarding the rights of Data Subjects in accordance with this Clause 7.

7.3 Even in the event of cooperation or support of the Customer by Jungheinrich, the Customer shall remain solely responsible and accountable for the fulfilment of the Data Subject Rights in relation to the Data Subjects.

8. DATA PROTECTION OFFICER

8.1 Where necessary, Jungheinrich has appointed a data protection officer who performs his or her duties in accordance with the provisions of the Applicable Data Protection Law.

8.2 Jungheinrich will provide the Customer with information on the person and contact details of the data protection officer upon request.

9. MAINTAINING CONFIDENTIALITY

9.1 When carrying out work on behalf of the Customer, Jungheinrich shall only employ persons who have undertaken to maintain confidentiality and who have been familiarised in advance with the relevant provisions of the Applicable Data Protection Law or who are subject to an appropriate statutory duty of confidentiality.

9.2 The Customer and Jungheinrich are obliged to treat as confidential all knowledge of business secrets and data security measures of the other party obtained within the scope of this Agreement ("**Obligation of Confidentiality**"). This Obligation of Confidentiality shall also apply in cases of remote access to Personal Data. It shall remain in force even after termination of this Agreement. If the Parties have agreed provisions on the Obligation of Confidentiality in the Main Contract, these shall apply accordingly to this Agreement. If the Parties have (instead or in addition) concluded a separate confidentiality agreement, this shall take precedence over the provision in this Clause 9.2.

9.3 The Parties are entitled to disclose information related to this Agreement or its implementation to external consultants to the extent necessary to comply with legal obligations or for legal defence and prosecution and to the extent that the external consultants are subject to contractual or statutory confidentiality obligations at least equivalent to the obligations under this Agreement.

10. CONTROL AND VERIFICATION OBLIGATIONS OF JUNGHEINRICH

10.1 Jungheinrich regularly monitors its internal processes and the technical and organisational measures in accordance with **Appendix 3** to ensure that the Processing in its area of responsibility is carried out in accordance with the requirements of the Applicable Data Protection Law and that the protection of the rights of the Data Subjects is ensured.

10.2 Jungheinrich shall present the technical and organisational measures taken to the Customer upon request within the scope of the Customer's rights of control in accordance with

Clause **Hiba! A hivatkozási forrás nem található.** of this Agreement.

11. SUB-PROCESSING RELATIONSHIPS

11.1 Jungheinrich is authorised to use Sub-processors.

11.2 A sub-processing relationship exists if Jungheinrich commissions Sub-processors to perform all or part of the service owed to the Customer under the Main Contract, which involves the Processing of Personal Data on behalf of the Customer. Jungheinrich will carefully select Sub-processors, paying particular attention to the technical and organisational measures taken by them, and will enter into agreements with them to the extent necessary to ensure appropriate data protection and information security measures.

11.3 The Customer agrees to the use by Jungheinrich of the Sub-processors listed in **Appendix 4**. Jungheinrich shall inform the Customer before involving additional Sub-processors or replacing the existing ones. The Customer may object to any such change in the Sub-processors within fourteen (14) days of notification of the change. The Customer should justify the objection and, in particular, will not make arbitrary use of its right of objection. If no objection is made within the time limit, consent to the amendment shall be deemed to have been granted. If the Customer objects to the change in sub-processing and if it is not possible for Jungheinrich to engage another Sub-processor under reasonable conditions at short notice, Jungheinrich shall be entitled either to adjust the agreed remuneration by the higher costs incurred by the alternative sub-processing or to terminate this Agreement and the Main Contract extraordinarily.

11.4 If Jungheinrich places orders with Sub-processors, Jungheinrich shall transfer its data protection obligations under this Agreement to the Sub-processor in accordance with the Applicable Data Protection Law to the applicable and reasonable extent. For this purpose, Jungheinrich shall enter into a corresponding agreement with the Sub-processor in written or text form and shall regularly monitor compliance with these obligations by the Sub-processor. Jungheinrich shall provide the Customer with a copy of such a sub-processing agreement and any subsequent amendments at the Customer's request. To the extent necessary to protect trade secrets or other confidential information, including Personal Data, Jungheinrich may obscure the wording of the agreement before providing a copy.

11.5 If a Sub-processor engaged by Jungheinrich fails to fulfil its data protection obligations, Jungheinrich shall be liable to the Customer for compliance with the obligations of that Sub-processor.

11.6 A sub-processing relationship within the meaning of this provision shall only exist for those services that are provided for the performance of or in direct connection with the main service for the Customer. This does not include so-called ancillary services that Jungheinrich receives from third parties in connection with the performance of its own business operations and where the third parties do not have access to the Customer's Personal Data, such as telecommunications services, technical maintenance services, user services and cleaning services. However, Jungheinrich is obliged to make appropriate contractual agreements and to take control measures to ensure the protection and security of the Customer's Personal Data, also in the case of such ancillary services.

12. CUSTOMER'S RIGHTS OF CONTROL

12.1 If there is a legitimate cause, the Customer has the right at any time, otherwise once every two years, and in consultation with Jungheinrich, to demand proof of Jungheinrich's compliance with this Agreement to the extent necessary and reasonable. In principle, Jungheinrich will prove compliance with this Agreement by submitting appropriate certification or other suitable documentation.

12.2 If the submission of a certification or other appropriate documents pursuant to Clause 12.1 is insufficient to prove compliance with this Agreement in individual cases, Jungheinrich shall, after joint coordination and a regular notice period of three (3) weeks, enable the Customer to carry out an on-site inspection of the Processing on behalf in accordance with this Agreement at Jungheinrich's business premises during Jungheinrich's normal business hours. The Customer shall only allow such checks to be carried out by sufficiently qualified internal or external audit personnel who are bound to secrecy. Persons who are to be regarded as competitors of Jungheinrich due to their profession or employment relationship are unsuitable for the audit. Jungheinrich does not have to allow audits by insufficiently qualified or unsuitable persons. The Customer will inform Jungheinrich of the persons who are to carry out the on-site audit at least one (1) week before the planned on-site audit.

12.3 The Customer shall pay Jungheinrich an Appropriate Expense-Related Remuneration for the expenses incurred by Jungheinrich in exercising the Customer's inspection rights.

12.4 Jungheinrich can, at its discretion, provide evidence in accordance with Clause 12.1 through compliance with approved rules of conduct in accordance with Art. 40 GDPR, certification in accordance with an approved certification procedure in accordance with Art. 42 GDPR, current certificates, reports or report extracts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors), suitable certification through IT security or data protection audits (e.g. in accordance with BSI basic protection) or comparable measures. Jungheinrich shall provide the Customer with appropriate proof in a suitable form and to an appropriate extent upon request.

13. NOTIFICATION AND BEHAVIOUR OF JUNGHEINRICH IN THE EVENT OF PERSONAL DATA BREACHES

13.1 Jungheinrich shall inform the Customer without delay if it becomes aware of any violations of the protection of the Customer's Personal Data or other breaches of data protection provisions or regulations of this Agreement. Jungheinrich shall take appropriate measures to secure the Personal Data and to mitigate any possible adverse consequences for the Customer or the Data Subjects and shall consult with the Customer to this end.

13.2 In the event of a Personal Data breach in connection with the data processed on behalf of the Customer, Jungheinrich shall, at the Customer's request, provide reasonable assistance to the Customer, taking into account the nature of the Processing and the information available to Jungheinrich, so that the Customer can fulfil its legal obligations to document and, if necessary, report and notify a Personal Data breach. In compensation for the expenses incurred by Jungheinrich in this respect, the Customer shall pay Jungheinrich an Appropriate Expense-Related Remuneration.

13.3 Jungheinrich shall inform the Customer without delay of control actions and other measures taken by supervisory or investigating authorities, insofar as the actions relate to this Agreement, unless Jungheinrich is prohibited from informing the Customer by the investigating authority. Upon request, the Customer and Jungheinrich shall cooperate with the supervisory or investigative authority in the performance of their duties.

13.4 Insofar as the Customer, for its part, is exposed to a control by a supervisory authority, administrative offence or criminal proceedings, the liability claim of a Data Subject or a third party or any other claim in connection with the Processing on behalf of the Customer by Jungheinrich, Jungheinrich shall support the Customer to the best of its ability to the extent possible and reasonable in the exercise of legal protection against such a measure or the defence against such claims. The expenses incurred by Jungheinrich in this connection shall be reimbursed to Jungheinrich under the conditions stipulated in the Main Contract.

13.5 The foregoing provisions shall continue to apply unchanged after the termination of this Agreement until the obligations regulated therein have been fulfilled in their entirety.

14. **Erasure and return of Personal Data after termination of the Agreement**

After termination of this Agreement, Jungheinrich shall, at the Customer's discretion, either delete all Personal Data still processed on behalf of the Customer and certify to the Customer at the Customer's request that this has been done, or return all Personal Data still processed on behalf of the Customer to the Customer and delete existing copies, unless Jungheinrich is legally authorised or obliged to store the Personal Data.

15. **Other Duties of Jungheinrich**

Upon request by the Customer in writing or text form, Jungheinrich is obliged to support the Customer to the extent required by the Applicable Data Protection Law

(a) in the fulfilment of Data Subject Rights,

(b) in the Customer's data protection impact assessment,

(c) in the context of prior consultations with the supervisory authority and

(d) in the preparation of the Processing activities by the Customer

in a reasonable manner, taking into account the type of data Processing and the information available to Jungheinrich. Even in the event of co-operation or support of the Customer by Jungheinrich, the Customer shall remain solely responsible and accountable for the actions or documentation referred to in letters (a) - (d).

Jungheinrich may demand Appropriate Expense-Related Remuneration for the support services mentioned in letters (a) - (d).

16. **Liability for breaches of data protection law**

Each party shall be liable to the Data Subjects in accordance with Applicable Data Protection Law. The Parties shall be liable for compliance with their obligations under this Agreement and to each other in accordance with the statutory provisions of the applicable law. In all other respects, the liability provisions of the Main Contract shall apply.

17. **Final provisions**

17.1 Amendments to this Agreement and ancillary agreements must be made in writing or with a qualified electronic signature. This also applies to the waiver of this formal requirement.

17.2 Should individual parts of this Agreement or its future amendments or supplements be or become wholly or partially void, invalid, voidable or unenforceable, this shall not affect the validity of the remaining provisions of this Agreement. In place of the void, invalid, voidable or unenforceable provision, an appropriate provision shall be applied which, as far as legally possible, comes as close as possible to what the Parties would have intended if they had known that the provision was void, invalid, voidable or unenforceable in whole or in part.

17.3 In the event of a conflict between this Agreement and the Main Contract, the provisions of this Agreement shall take precedence over the Main Contract with regard to the obligations relating to the Processing of Personal Data in the context of the data Processing described in **Appendix 2** to this Agreement.

18. **List of Appendices**

The following appendices are an integral part of this Agreement:

- **Appendix 1**: Template letter of accession
- **Appendix 2** : Details of data Processing on behalf of the Customer
- **Appendix 3** : Technical and organisational measures
- **Appendix 4** : Sub-processors

Appendix 1

Appendix 1 - Template letter of accession

From: [*Name of the company to accede to the Agreement*]
[address]

To: [*name of the company to receive the letter of accession*]
[*address*]

[*Date*]

ACCESSION TO THE DATA PROCESSING AGREEMENT FOR JUNGHEINRICH DIGITAL PRODUCTS AND SOFTWARE SOLUTIONS

We refer to the Data Processing Agreement for Jungheinrich Digital Products and Software Solutions ("**Agreement**") dated *[date of conclusion of contract]* between [*insert company of the Customer*] and [*insert Jungheinrich company with which the Main Contract was concluded*].

Pursuant to Clause 3.2 of the Agreement, we hereby accede to the Agreement for the products and services specified in the *[insert contract name]* dated [*insert date*] ("**Main Contract**") on the terms and conditions set out in Clause 3 of the Agreement with effect from *[insert date of accession]*, to the extent that the services of the Main Contract involve or relate to the Processing of Personal Data.

For: [*name of the acceding company*]

Name: _____

Function: _____

Place, Date: _____

Signature: _____

Appendix 2

Appendix 2 - Details of data Processing on behalf

This **Appendix 2** contains further information on the details of data Processing by Jungheinrich on behalf of the Customer in the context of the provision of Digital Products and Software Solutions from Jungheinrich and the provision of maintenance and support services in relation to Digital Products and Software Solutions from Jungheinrich, in particular on the type and purpose of data Processing and the categories of Personal Data and Data Subjects concerned. The information is specified for each of Jungheinrich's Digital Products and Software Solutions that the customer has purchased under the Main Contract.

Annex toAppendix 2	**Digital Products and Software Solutions from Jungheinrich**
Annex A	**Fleet Management Solutions**

Appendix 2 Annex A

Annex A – Jungheinrich Fleet Management Solution (FMS)

Jungheinrich offers various fleet management solutions. This**Annex A** to**Appendix 2** describes the details of data Processing by Jungheinrich on behalf of the Customer of the provision of the fleet management solutions named in this Annex, in particular the type and purpose of data Processing (see Clause 1), the categories of Personal Data affected by the Processing (see Clause 1.2) and the categories of Data Subjects affected by the Processing (see Clause 3).

In some cases, these solutions can be ordered with different service packages ("**bundles**"). The selection of the bundles by the Customer is recorded in the Main Contract.

1. **TYPE AND PURPOSES OF DATA PROCESSING**

1.1 **Jungheinrich FMS**

In the course of providing the Jungheinrich FMS, Jungheinrich Processes the Personal Data provided by the Customer or collected for the Customer in the course of providing the service or Processed in any other way for the purposes set out below on the Customer's behalf.

The Processing of Personal Data of the users of the Jungheinrich FMS Online Portal provided by Jungheinrich, which takes place in the context of the use of the portal, is not covered by the Processing on behalf of the Customer. This Processing is carried out under the sole responsibility of Jungheinrich.

When the Jungheinrich FMS provided by Jungheinrich is used by the Customer, (machine) data is generated which may relate to an identified or identifiable natural person and the Processing of which in this case is subject to the provisions of data protection law. Jungheinrich collects and stores this data on behalf of the Customer in order to enable the contractually agreed use of the fleet management system. The purpose of the Processing is therefore the collection, analysis and evaluation of data from the Customer for the purpose of controlling and managing its vehicle fleet.

The entry of data other than the relevant data mentioned in this Annex is not required, but may be provided by the Customer at its own responsibility. In this case, the Customer is solely responsible for ensuring the lawfulness of the Processing through appropriate measures in the internal relationship with its employees.

The Jungheinrich FMS is divided into different Bundles that are purchased individually by the Customer. The respective purposes as well as the data Processed in each case are described below according to the bundle.

(a) **Starter Bundle**

The Starter Bundle includes an inventory function that is used to digitise warehouses. This provides a platform for the digitisation of warehouses. This allows internal serial numbers and unit names to be assigned and managed, and additional units to be added.

The operating hours function of the Starter Bundle enables optimization of fleet capacity. This is done on the basis of forecasts at the fleet, vehicle and contract data.

By assigning vehicles and devices to individual users and user groups or drivers and driver groups, it may be possible to establish a relation to an identified or identifiable natural person.

(b) **Finance Bundle**

The Finance Bundle offers transparency by displaying the costs for individual vehicles as well as for the entire fleet over the course of a defined time period chosen by the user. The analysis function determines the respective costs per operating hour and displays them over individually selectable time periods and historical trends in the cost module of the Finance bundle. For the analysis, invoices, service reports as well as equipment data are being taken into account. These usually contain Personal Data. In addition, this bundle offers transparency about service reports of individual vehicles. This allows to have an overview over the conducted services for the fleet. In addition to this, this bundle also shows an overview over upcoming and conducted maintenance services. Furthermore, the bundle includes a possibility to visually track cost outliers by setting individual limits which need to be monitored.

(c) **Safety Bundle**

The Safety Bundle includes the shock management function and the Pre-Op Check module and helps to increase safety in the warehouse.

The Access Management is used to protect the fleet from unauthorised use. The vehicles are started using a transponder card. It is possible to individually determine which vehicles may be used with a transponder card for an individual driver. The authorisation can refer to the driving licence, the job assignment and the vehicle type.

The driver deployment function provides an overview of the utilisation of the industrial truck fleet. The vehicles are put into operation using a transponder card. The overview consists of the switch-on and -off times of the vehicles, which are enriched with additional information, namely data on the vehicle users and the vehicle, in order to provide the users with a holistic overview of the use of the vehicle fleet and to detect possible misuse. It is possible to determine the respective driver and the associated transponder card for each use of the vehicle.

The departure control function is used for status queries on the industrial trucks by the driver in order to increase safety in the warehouse. Depending on the components installed in the vehicles, single-stage (visual inspection) or two-stage (visual and functional inspection) queries are possible. The departure control can be activated individually for each industrial truck and is carried out after successful login using a transponder card on a display device of the respective industrial truck. In the event of a negative departure control, e.g. due to a detected defect, the system does not restrict the usability of the affected industrial truck for the driver.

An overview shows all departure controls carried out including the respective result ("successful" or "unsuccessful"). The history of the departure controls carried out is enriched with additional information (e.g. time, vehicle number, driver ID) in order to identify vehicle defects at an early stage and to avoid consequential damage or safety risks for employees. The employees who carry out the respective departure control on an industrial truck are displayed without being identified by name when using the default setting. However, the Customer can also select a display with a real name in the settings.

The shock management function provides data on shocks and offers configurable truck reactions (e.g. crawl speed). The module Pre-Op Check provides the configuration of checklists for visual and functional truck inspections, including configurable truck reactions for critical questions (e.g. crawl speed). The checklists can be assigned to individual trucks and must be completed by the driver at configurable points of time. As a prerequisite for setting the truck into operations mode, the driver must complete the checklists after a successful login with the transponder card. The history of the visual and functional checks carried out is enriched with additional information (e.g. time, vehicle number, driver ID) and is provided in a table view in the reports section. A detail view in the reports offers information about the specific responses to each question of every completed check. As per default, the reports of the checks are displayed without a driver name. However, the Customer can also select to display the report including driver's name in the settings.

The shock management function and the Pre-Op Check module are used together with access control. Thus, the Access Module is already included in the Safety Bundle.

In combination with the Finance Bundle, the Safety Bundle also includes the Location Analysis module. The Location Analysis module enables FMS users to efficiently analyze their fleet data from existing modules across multiple locations in an aggregated view. It

Appendix 2 Annex A

allows to perform cross-location analytics with data presented from a country-wide, location group, or individual location perspective.

(d) **Safety & Performance Bundle**

The Safety & Performance Bundle combines the functionalities of the Safety Bundle and the Productivity Module. Thus, it provides data of shocks, enables the creation of checklists for visual and function checks (Pre-Op Check), offers configurable vehicle reactions (e.g. crawl speed) and provides an overview of the various utilizations of the Customer's fleet. The data for determining the utilization refers to the operating times of the vehicles.

The Productivity Module provides an overview of the various capacities of the industrial truck fleet and the Customer's fleet. The Customer has the option of viewing both the parallel load and the peak load. Capacity is determined by processing the operating times of the vehicles.

(e) **Energy Bundle**

The Energy bundle provides energy-related insights based on the state of charge values of the Customers' electric trucks which are equipped with a Jungheinrich telematics box. This allows to analyze the current usage pattern of the batteries in order to derive potential measures to maximize efficiency and battery lifetime. In case the access management function is activated, the data displayed in this bundle can potentially be connected to the driver.

1.2 **Jungheinrich FMS API**

The Jungheinrich FMS API is used for data exchange between the Jungheinrich FMS platform and the customer’s IT system so that the data can be used in the customer’s BI systems and for creating comprehensive reports.

Depending on the purchased Jungheinrich FMS bundles, the data that is made available for the customer divers. The data set consists of vehicle and location data, operating costs, operating hours, shock management, employee and/ or access management data.

Appendix 2 Annex A

2. CATEGORIES OF PERSONAL DATA

The following categories of Personal Data are processed for the provision of the fleet management solutions selected by the Customer in the Main Contract:

Categories of Personal Data	Jungheinrich FMS					
	Starter Bundle	Finance Bundle	Safety Bundle	Safety & Performance Bundle	Energy Bundle	Jungheinrich FMS API
Basic personal information	x	x	x	x	x	x
Communication data	x	x	x	x	x	x
Log data	x	x	x	x	x	x
Vehicle user data			x	x	x	x
Vehicle data			x	x	x	x
Medical data			(x)*	(x)*		

The above-mentioned data categories generally include the following data, which can be provided by the Customer and processed by Jungheinrich for the provision of services:

- Basic personal information (e.g. first name, middle initial, last name, signature, personnel number)
- Communication data (e.g. login email address, telephone number, API key)
- Log data (e.g. logging of logon and logoff times that have occurred, as well as logging of capture and modification times, IP address, configuration changes in the management portal, date and time of logon and logoff of a driver to a specific vehicle including the final state of the vehicle, multi-login)
- Vehicle user data (e.g. first name, last name, transponder ID, vehicle licence class, driving licence number, licence expiry date, driver experience level, logon information, access ID, PIN, external ID, authorisation, expiry date, group assignment, driving times, shock messages of the vehicle they operate)
- Vehicle data (e.g. vehicle ID, vehicle segment, speed, lifting events (lifting and lowering), battery level, vehicle type, deployments, shocks, total number of shocks during deployment, driver checklists completed, departure check result on vehicle condition)
- Medical data (* Module Pre-op Check: by default, there are no system-suggested checklists implemented, therefore no Processing of medical data is intended. Customers may create and use individual checklists at their own discretion. This may include the collection and Processing of medical data, which remain under sole responsibility of the Customer in accordance with Section 1.4 of the Agreement. For further information please refer to 1.1(c) and 1.1(d) of this Annex.)

The fleet management solutions provided by Jungheinrich are regularly adapted and updated to meet new technical and legal requirements. This may result in changes to the categories of Personal Data processed in the individual fleet management solutions. An up-to-date overview of the categories of data processed can be accessed via the following link: https://jungheinrich.com/processing-of-personal-data-in-jungheinrich-digital-products-1136138.

3. CATEGORIES OF DATA SUBJECTS

For the provision of the fleet management solutions specified by the Customer in the Main Contract, Personal Data of the following categories of Data Subjects are processed:

Categories of Data Subjects	Jungheinrich FMS					
	Starter Bundle	Finance Bundle	Safety Bundle	Safety & Performance Bundle	Energy Bundle	Jugnheinrich FMS API
Users	x	x	x	x	x	x
Drivers			x	x	x	x
Signatories of service reports		x				

The fleet management solutions provided by Jungheinrich are regularly adapted and updated to meet new technical and legal requirements. This may result in changes to the categories of Data Subjects processed in the individual fleet management solutions. A current overview of the categories of Data Subjects can be accessed via the following link: https://jungheinrich.com/processing-of-personal-data-in-jungheinrich-digital-products-1136138.

4. REGULAR STORAGE PERIOD

Jungheinrich will store the Personal Data processed in the context of the provision of the fleet management solutions specified by the Customer in the Main Contract only for as long as is necessary for the purposes for which it is processed and in a form which permits identification of Data Subjects, unless storage beyond this period is necessary for compliance with a legal obligation to which Jungheinrich is subject or for the establishment, exercise or defence of legal claims.

The regular storage periods for Personal Data and the main non-Personal Data are described below:

Appendix 2 Annex A

Table with regular storage period of Personal Data within the Jungheinrich FMS

Customer data	Storage period	Bundles concerned
Name of the logged-in user in audit logs	18 months	All available bundles
Names of drivers and transponder IDs in access management	Until the end of the contract or expiry of the licence or until manual deletion by the Customer	Safety Bundle, Safety & Performance Bundle
Names of drivers and transponder IDs in operation reports	6 months	Safety Bundle, Safety & Performance Bundle
Names of drivers and transponder IDs in pre-op check and quick check reports	6 months	Safety Bundle, Safety & Performance Bundle
Names of drivers and transponder IDs in shock reports	6 months	Safety Bundle, Safety & Performance Bundle
Name and signature of the signatories in the service reports (PDF files)	Maximum 2 years and 36 days. PDF files are available from 1 January of the previous year to the current day.	Finance Bundle

Optional if there is a contractual Agreement on the use of the FMS API (interface):

Customer data	Storage period	Justification of a storage period over 5 years
FMS API basic data: Customer, location, equipment, tags (attributes), licenses	Until the end of the contract or expiry of the licence	Necessary for the provision of the interface / API
API key management (incl. audit logs)	Until the licence expires	Necessary for the provision of the interface / API

Appendix 3

Appendix 3 - Technical and organisational measures

Jungheinrich has taken the following technical and organisational measures ("**TOMs**") to ensure a level of protection appropriate to the risk to the rights and freedoms of natural persons. Jungheinrich regularly reviews, assesses and evaluates the effectiveness of the TOMs to ensure the security of the Processing and adapts the TOMs as necessary to ensure a consistently high level of protection.

The TOMs taken by Jungheinrich vary with regard to the types of Digital Products and Software Solutions due to the differences in factual, technical and organisational aspects between the different types of Digital Products and Software Solutions.

Annex toAppendix 3	**Technical and organisational measures**
Annex A	Technical and organisational measures for Jungheinrich Fleet Management Solutions

Appendix 3 Annex A

Annex A - Technical and organisational measures for Jungheinrich Fleet Management Solutions

1. Confidentiality

1.1 Access control

The following measures are taken to ensure that unauthorised persons are prevented from entering the building or the rooms in which the Processing systems are located with which Personal Data are Processed or used:

- Binding procedure for assigning and passing on access authorisations to the building, the offices and the data centres
- Access control system (access card)
- Central key management
- Employee ID cards with photo
- Design of computing centres as closed security areas
- Electronic code locks to the rooms of the Processing facilities
- Guideline for accompanying visitors
- Logging of persons entering and exiting
- Security guard service (building protection outside office hours)
- Burglar alarm system
- Video monitoring in the data centres and/or sensitive areas of the building
- Secured entry
- Burglar-resistant windows
- Locking of cabinets and offices when absent

1.2 Physical access control

Measures to prevent Processing systems from being used by unauthorised persons:

- Access only after identification and authentication
- Binding procedure for issuing access authorisations
- Clear assignment of user accounts and users
- Policy for secure and proper handling of passwords
- Automatic locking of user account after defined number of failed login attempts or after defined inactivity
- Automatic locking of computer after defined inactivity with subsequent re-login
- Automatic standby operation of local computers
- Access logging and incident-related analysis of log files
- Controlled deletion of Personal Data after expiry of Agreement
- Regular vulnerability analysis for Web applications
- Regulations for mobile Processing systems or data carriers (encryption of hard drives/data carriers, guideline for handling mobile devices/data carriers, possibility for remote erasure on smartphones)

1.3 Access control

Measures to ensure that those authorised to use a Processing system can only access the data which is subject to their access authorisation and that Personal Data cannot be read, copied, modified or removed without authorisation during Processing, use and after storage:

- Organised roles and authorisations concept
- Binding procedure for issuing access authorisations
- Periodic review of existing authorisations
- Access logging and incident-related analysis of log files
- Differentiated folder concept (clear naming convention for files)
- Adjustment of security-relevant default settings of new IT systems and applications and deactivation of non-required security-relevant programs and functions
- Clear labelling and secure storage of data carriers
- Secure erasure of data
- Clear Desk/Clear Screen Policy
- Access-safe archiving of data
- Sensitive Personal Data shall be stored in encrypted form in compliance with common security standards

1.4 Separation controls

Measures to ensure that data collected for different purposes can be Processed separately:

- Logical separation by means of access rules
- Software-based multi-client capability
- Access to data records only via applications that satisfy the separation requirement
- Separation of production and test systems
- Linking records to a specific purpose

1.5 No attribution by name

Measures to ensure that no reference to persons can be established from the data:

- Evaluations in the application are possible "by default" without reference to persons
- Possibility of an evaluation without attribution of names by the Customer

2. Integrity

2.1 Transfer control

Measures to ensure that Personal Data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or while being transported or stored on data carriers, and that it is possible to verify and establish to which bodies Personal Data are intended to be transmitted by data transmission equipment:

- Encrypted communication over insecure networks according to common security standards
- Secure disposal of data carriers that are no longer needed

Appendix 3 Annex A

- Possibility of electronic signature for personal e-mail communication
- Logging of the retrieval and transmission of Personal Data
- Prohibition on the use of unapproved hardware and software
- No forwarding of information to external IT services (private email addresses, non-shared cloud storage)
- Guidelines for employees regarding the printing of sensitive documents
- Guidelines for staff regarding the use of data carriers

2.2 **Input control**

Measures to ensure that it is possible to check and establish retrospectively whether and by whom Personal Data have been entered into, modified or removed from Processing systems:

- Access to Processing systems only possible after login
- No disclosure of passwords (password policy)
- Guideline on how to proceed if a password becomes known (password guideline)
- Automatic logging of the entry, modification and erasure of Personal Data
- Incident-related analysis of log files

3. **Availability and resilience**

3.1 **Availability control**

Measures to ensure that Personal Data is protected against accidental destruction or loss and is available:

- Documented backup and recovery concept with regular backups and disaster-proof storage of data carriers
- Use of security controls such as antivirus and firewall
- Storage systems with redundancy
- Separate storage of data
- Protection against fire, overheating, water damage, overvoltage and power failure in the server room
- Use of uninterruptible power supply and emergency generators
- Emergency concept in place (including regular review of effectiveness)
- Binding workflow for performing updates
- Monitoring of systems to detect faults
- Defined rules on representation (especially for privileged accounts)
- Procedures for regular review, assessment and evaluation

3.2 **Data protection management**

Measures to ensure that the TOMs taken remain effective in the long term:

- Regular control of the TOMs taken
- Evaluation of messages and reports on unusual incidents
- Training of employees in the use of IT and raising IT security awareness
- Regular professional training of the IT officers and the company data protection officer

3.3 **Privacy-friendly default settings**

Measures to ensure that privacy-friendly technology design contributes to compliance with the principles of data protection and that data is only Processed to the extent necessary on the basis of privacy-friendly default settings:

- Privacy by design
- Organisational assurance that communication and notification obligations are fulfilled
- Data Subjects may exercise their right to object to Processing (e.g. advertising) by means of automated procedures.
- Privacy by default
- Privacy-friendly default settings in relation to the amount of Personal Data collected
- Privacy-friendly default settings in relation to the scope of Processing
- Privacy-friendly default settings with regard to compliance with storage and erasure periods

3.4 **Order control**

Measures to ensure that Personal Data Processed on behalf of the Customer is only Processed in accordance with the Customer's instructions:

- Processing of Personal Data of the Customer by Jungheinrich is only carried out for internal purposes within the framework of the customer relationship
- Ensuring Processing on behalf of the Customer in accordance with instructions by demarcating responsibilities between the Customer and Jungheinrich
- Changes ordered by the Customer, which are to be carried out by Jungheinrich, are subject to the specifications of order control
- Pre-established criteria for the selection of Sub-processors shall be stringently adhered to
- Jungheinrich employees only have access to the information they need to carry out the order
- Commitment of Jungheinrich personnel to the data protection principles of the applicable law, in particular the confidentiality of data
- Control of the execution of the contract shall be ensured

4. **Remote access**

Clauses 1 to 3 of this**Annex A** to**Appendix 3** also apply to the extent applicable in the event of remote access to Personal Data.

Appendix 4

Appendix 4 - Sub-processors

For the Processing of Personal Data on behalf of the Customer, Jungheinrich utilises the services of third parties who process Personal Data on its behalf ("Sub-processors"). These can be found in the following overview.

The Sub-processors used by Jungheinrich vary with regard to the types of Digital Products and Software Solutions due to the differences in factual, technical and organisational aspects between the different types of Digital Products and Software Solutions.

Annex toAppendix 4	**Sub-processors**
Annex A	Sub-processors for Jungheinrich Fleet Management Solutions

Appendix 4 Annex A

Annex A - Sub-processors for Jungheinrich Fleet Management Solutions

Sub-processor (Name, legal form, registered office of the company)	**Type of service provided**	**Processing location** (Location of data Processing or location of data access)
Jungheinrich AG Information Technology Friedrich Ebert Damm 129, 22047 Hamburg, Germany	• Service Hosting	Server locations: • Hamburg, Germany (Jungheinrich AG IT) • Frankfurt, Germany (Equinix Germany GmbH)
Jungheinrich Digital Solutions AG & Co.KG Sachsenstr. 20, 20097 Hamburg, Germany	• Development • Maintenance & Support • IT Administration	
Jungheinrich Digital Solutions S.L. Calle Gran Via nº 30 - Planta 7, 28013 Madrid, Spain	• Development • Maintenance & Support • IT Administration	
Jungheinrich Business Services Romania S.R.L. Brasov, Saturn Blvd. No. 51, 5th floor, 105440 Brasov county, Romania	• IT Administration • Support	
Jungheinrich Business Services Croatia d.o.o. Vjekoslava Heinzela 70 10000 Zagreb, Croatia	• Development • Maintenance & Support • IT Administration	
Jungheinrich Svenska AB Starrvägen 16 232 61 Arlöv, Sweden	• Development • Maintenance & Support • IT Administration	
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg	• Service Hosting	Server locations: • Frankfurt, Germany • Dublin, Ireland • Paris, France • Stockholm, Sweden • Milan, Italy
Splunk Services Germany GmbH Salvatorplatz 3, 80333 Munich, Germany	• Storage and Processing of log data	Server location: • Frankfurt, Germany
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin, Ireland	• Service hosting (provision of integrated services, in particular for access control and for data analysis and evaluation)	Server locations: • West Central Europe (Germany) • West Europe (Netherlands) • North Europe (Ireland)
Device Insight GmbH Willy-Brandt-Platz 6, 81829 Munich, Germany	• IoT service (provision of IoT interface)	
ClickHouse, Inc. 650 Castro St., Suite 120 #92426, Mountain View CA 94041, USA	• Cloud-based data analysis and evaluation	Server location: • Frankfurt, Germany
Widas ID GmbH Maybachstraße 2, 71299 Wimsheim, Germany	• CIAM	Server location: • Germany