Data Processing Agreement
for

Digital Jungheinrich Products

(hereinafter referred to as the "**Agreement**")

between

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

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

PREAMBLE

A. The Parties have concluded a contract for the provision of Digital Jungheinrich Products (hereinafter referred to as "**Main Contract**"). As part of the provision of Digital Jungheinrich Products, Jungheinrich processes/may process personal data on behalf of the Customer to the extent described in **Appendix 2 to Appendix 4**, thus Parties enter into this present Agreement.

B. This Agreement is an integral part of the Main Contract and forms an appendix to it.

1. DEFINITIONS

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

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

1.2 "**Processor**" means a natural or legal person, public authority, agency or other body which Processes personal data on behalf of the controller. Jungheinrich is the Processor within the scope of its Processing of personal data on behalf of the Customer to the extent regulated in this Agreement.

1.3 "**Data Subject**" means the person to whom personal data refers.

1.4 "**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).

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

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

1.7 "**Sub-processor**" (**additional data-processor**): means an additional Processor or Processors within the meaning of Art. 28 (2), (4) GDPR.

1.8 "**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.

1.9 "**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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10 "**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.

2. SUBJECT AND TERM OF THE AGREEMENT; APPLICABLE LAW

2.1 Subject of the Agreement

The subject of this Agreement is the Processing of personal data by Jungheinrich (as a Processor) on behalf of the Customer (as a Controller) in accordance with the provisions of the Main Contract. Data Processing operations under Jungheinrich's own responsibility remain unaffected by this Agreement. See also Clause 4.5.

2.2 Term of the Agreement; Termination

The term of this Agreement shall be the term of the Main Contract.

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

2.3 Applicable law

The provisions of the GDPR, the relevant national regulations for the implementation and introduction of the GDPR (especially the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information), all other data protection laws at the registered office of the Parties, the guidelines and guidance of the competent supervisory authorities (especially the National Authority for Data Protection and Freedom of Information – NAIH) as well as the legally binding data protection decisions of the competent courts (collectively "**Applicable Data Protection Law**") shall be authoritative for the data protection provisions of this Agreement and their interpretation.

The law applicable 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 shall each enter into this Agreement in their own name as well as in the name and on behalf of their Affiliates, to the extent that a corresponding authorization exists, whereby a separate data processing agreement is concluded between the relevant Affiliate of the Customer and the relevant Affiliate of Jungheinrich in each case. Each Affiliate of the Customer involved in this way is hereby bound to comply with the requirements of this Agreement and, to the extent applicable, the Main Contract and shall have the rights and obligations of a Controller under this Agreement. As a result of this provision, the Involved Affiliates do not become a party to the Main Contract, but only a party to this Agreement. The Parties are obliged to document the existence of proper authorisation and to prove it in a suitable form at the request of the respective other Party. For the purpose of documenting the Affiliates that are party to this Agreement, the Parties will exchange and update, as necessary, a list of the Involved Affiliates.

3.2 Subsequent accession

An Affiliate of the Customer who is not a party to this Agreement at the time of conclusion of the contract may accede to this Agreement at any time by signing a declaration of accession in accordance with the template in **Appendix 1** and sending it to Jungheinrich. In the event that Jungheinrich does not object to the accession within two (2) weeks by notification in text form, the acceding Affiliate shall become a party to this Agreement and shall henceforth have the rights and obligations of a Customer 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.

In the event that an Affiliate on the part of Jungheinrich is to take over the Processing activity in its entirety or in a contracting country, the above provision shall apply mutatis mutandis with the proviso that the acceding Affiliate of Jungheinrich informs the Customer or the Involved Affiliate or Affiliates of the Customer for which it will take over the Processing activities by means of a corresponding notice (instead of using the template declaration of accession).

3.3 Communication

The Customer, which is a Party to the Main Contract, shall coordinate the communication of its Involved Affiliates to Jungheinrich under this Agreement and shall be solely responsible for the communication with Jungheinrich under this Agreement. Jungheinrich may require that communication to Jungheinrich be made exclusively by the Customer and not by the Involved Affiliates.

3.4 Collective exercise of rights

Unless the exercise of any right or remedy under this Agreement by the Involved Affiliate on the part of the Customer itself is required by law, 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 under Clause 12. 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. SUBJECT OF AGREEMENT

4.1 Scope, type and purpose of Processing

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**, **Appendix 3** and **Appendix 4**.

4.2 Place of Processing

In principle, all contractually agreed Processing shall take place in a member state of the European Union (EU) or in another contracting state of the Agreement on the European Economic Area (EEA).

Any transfer of data by Jungheinrich to 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 EU law or the law of an EU Member State to which Jungheinrich is subject (in this case Hungary) 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

- a decision of the European Commission is available, according to which 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 recognized transfer mechanism within the meaning of Chapter V of the GDPR applies.

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

4.3 Categories of personal data

The categories of personal data Processed by Jungheinrich on behalf of the Customer depend on the Digital Jungheinrich Product which the Customer chosen under the Main Contract. An overview of the personal data Processed under this Agreement can be found in **Appendix 2**.

4.4 **Categories of Data Subjects**

The Data Subjects of the Processing by Jungheinrich are listed in **Appendix 3**.

4.5 **No data processing takes place**

Insofar as Jungheinrich collects and further processes (a) personal data on the use by the Customer of the applications, tools, platforms, software or hardware provided by Jungheinrich and/or (b) non-personal machine data relating to the Jungheinrich vehicles or machines used by the Customer (e.g. login data for the discharge of maintenance cycles, information on access to websites or dashboards, etc.), the Processing is carried out in this respect in Jungheinrich's own interest and for Jungheinrich's own purposes (IT security, analysis, product development and improvement). Jungheinrich is Controller with regard to this Processing. The Jungheinrich Digital Products Privacy Policy is available here: Adatvédelem digitális szolgáltatások (jungheinrich.hu).

5. TECHNICAL AND ORGANISATIONAL MEASURES

5.1 Jungheinrich shall apply the technical and organisational measures listed in **Appendix 5** in accordance with the Customer's instructions in order to ensure a level of protection appropriate to the risk of the Processing with regard to the confidentiality, integrity, availability and resilience of the systems and to establish the security of the 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.

Technical and organisational measures are subject to technical progress and development. In this respect, Jungheinrich is permitted to implement alternative adequate measures as long as the safety level of the determined measures is not undercut. Jungheinrich will document significant changes by amending **Appendix 5**.

5.2 Insofar as an audit by the competent data protection authority reveals a need for amendment 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 amend **Appendix 5** accordingly.

6. CUSTOMER'S AUTHORITY TO ISSUE INSTRUCTIONS

6.1 Within the scope of this Agreement, Jungheinrich will 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 a designated place 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 any verbal instructions in writing or electronically.

6.3 Jungheinrich will not use the personal data Processed on behalf of the Customer for any purposes other than those agreed, in particular for its own purposes or the purposes of third parties. No copies or other duplicate copies will be created without the Customer's knowledge. This does not apply to back-up copies, insofar as they are necessary to ensure proper Processing, or to personal data that is required in order to comply with statutory retention obligations.

6.4 Jungheinrich will immediately inform the Customer if it believes that an instruction on Processing would constitute a breach of applicable law. Jungheinrich is entitled to suspend the implementation of the corresponding instruction until it is confirmed or changed by a person responsible on the part of the Customer.

6.5 The Customer guarantees that the instructions given to Jungheinrich for the Processing of personal data comply with applicable law. The Customer indemnifies Jungheinrich against any claims by third parties as a result of non-compliance with this guarantee.

6.6 The Customer and Jungheinrich shall each designate to the other Party those persons (and their deputies) who are authorised to issue instructions or receive instructions in accordance with this Agreement. Unless otherwise agreed by the Parties, these persons shall be the same as the operational contacts and no further specific designation shall be necessary, otherwise the designation shall be made in text form or writing and in each case via the usual means of communication between the Parties.

6.7 If an instruction goes beyond the services agreed in the Main Contract, Jungheinrich can request an appropriate payment for its performance.

6.8 Insofar as Jungheinrich Processes personal data on its own responsibility (see Clause 0), Jungheinrich is not bound by the Customer's instructions.

7. RECTIFICATION, ERASURE AND RESTRICTION OF PROCESSING OF PERSONAL DATA

7.1 Insofar as a Data Subject raises a statutory claim directly against Jungheinrich for information, rectification, erasure, restriction of Processing, data portability, objection and injunction of a decision based exclusively on an automated individual decision-making regarding its personal data Processed by Jungheinrich on behalf of the Customer (together: "**Data Subject Rights**"), Jungheinrich shall forward this request to the Customer immediately. Jungheinrich shall only rectify, erase or restrict its Processing of the personal data of the Data Subject making the claim following a documented instruction from the Customer. The same shall apply to satisfying the right of the Data Subject to data portability and access. This does not apply to any Processing by Jungheinrich due to official or court orders in connection with the Data Subject Rights.

7.2 The costs incurred by Jungheinrich as a result of its assistance to the Customer in safeguarding the Data Subject Rights in accordance with this Clause 7 shall be reimbursed based on expenses on the basis of the terms agreed between the Parties in the Main Contract.

8. DATA PROTECTION OFFICER

8.1 Jungheinrich has appointed a data protection officer, to the extent necessary, who carries out his work in accordance with the provisions of the Applicable Data Protection Law.

8.2 Jungheinrich will provide the Customer, upon request, with information regarding the person and the contact details of the data protection officer. The Customer shall be informed of any change of the data protection officer after the information referred to in sentence 1 has been provided.

9. MAINTAINING CONFIDENTIALITY

9.1 When carrying out work on behalf of the Customer, Jungheinrich shall only utilise employees who have undertaken to maintain confidentiality and who have previously been familiarised with the provisions of the Applicable Data Protection Law relevant to them.

9.2 The Customer and Jungheinrich are obliged to treat all knowledge of business secrets and data security measures of the other Party obtained within the framework of the contractual

relationship as confidential. The regulations on confidentiality in Jungheinrich's T&Cs apply. The obligation to confidentiality also applies in cases of remote access to the personal data. It shall remain in force after the termination of this Agreement. If the Parties have concluded a separate confidentiality agreement, this shall take precedence over the provisions of Clause 9.2.

9.3 The Parties shall be entitled to disclose information related to this Agreement or its performance to their Affiliates and also to external advisors to the extent necessary to comply with legal obligations or for legal defence and prosecution and to the extent that the external advisors are subject to contractual or statutory confidentiality obligations at least equivalent to the obligations under this Agreement.

10. CONTROL AND VERIFICATION OBLIGATION OF JUNGHEINRICH

10.1 Jungheinrich regularly controls its internal processes as well as the technical and organisational measures in accordance with **Appendix 5** 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 according to Clause 12 of this Agreement.

11. SUB-PROCESSORS

11.1 Jungheinrich is entitled to utilise Sub-processors.

11.2 A sub-processing relationship exists if Jungheinrich commissions Sub-processors to perform all or part of the service 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 6**. 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 will transfer its data protection obligations under this Agreement to the Sub-processor in accordance with the Applicable Data Protection Law to the applicable and appropriate extent. To this end, Jungheinrich will conclude a corresponding agreement with the Sub-processor in text form and regularly monitor the Sub-processor's compliance with these obligations.

11.5 A sub-processing relationship within the meaning of this provision shall only exist for such services which 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 will enable the Customer to conduct an on-site audit of the Processing on behalf of the Customer pursuant to this Agreement at Jungheinrich's business premises during Jungheinrich's normal business hours after joint coordination and an advance notice period of three (3) weeks. The Customer shall only have such audits carried out by sufficiently qualified internal or external auditing personnel who are bound to secrecy. Persons who are to be regarded as competitors of Jungheinrich due to their profession or employment relationship are shall not be allowed to participate 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 reimburse Jungheinrich for its expenses incurred as a result of the exercise of the Customer's rights of control to a reasonable amount on the basis of the conditions agreed between the Parties in the Main Contract, taking into account Jungheinrich's financial expenses.

12.4 Jungheinrich can provide evidence of such measures, which relate not only to the specific Processing on behalf of the Customer, at its discretion by complying with approved codes of conduct pursuant to Art. 40 of the GDPR, certification in accordance with an approved certification procedure pursuant to Art. 42 of the GDPR, current test certificates, reports or report extracts from independent bodies (e.g. accountants, auditing department, data protection officers, IT security department, data protection auditors, quality auditors), suitable certification by IT security or data protection audits or comparable measures. Jungheinrich will make appropriate proof of this available to the Customer on request in a suitable form and to an appropriate extent.

13. NOTIFICATION AND BEHAVIOUR OF JUNGHEINRICH IN CASE OF VIOLATIONS

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 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.

13.3 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.

13.4 The foregoing provisions shall continue to apply unchanged after the termination of this Agreement until the relevant obligations have been fully performed.

14. ERASURE AND RETURN OF PERSONAL DATA

14.1 Jungheinrich shall, by default, enable erasure of the Customer's data within six (6) months after the end of the term of this Agreement in accordance with data protection requirements. The Customer can demand that Jungheinrich hand over to it at an earlier point in time all documents that have come into Jungheinrich's possession, Processing and usage results that have been produced as well as data files that are connected with the contractual relationship or erase them in accordance with data protection law or destroy them in an manner appropriate to data protection. If the Customer exercises its right in sentence 2, it shall reimburse Jungheinrich for all reasonable expenses incurred on the basis of the conditions agreed between the Parties in the Main Contract.

14.2 Jungheinrich is entitled to retain copies of the documents, created Processing and usage results as well as data files that have come into its possession, insofar as and to the extent that this is necessary for the fulfilment of Jungheinrich's statutory retention obligations (e.g. from tax law or for accounting and settlement purposes) or for the assertion, exercise or defence of legal claims.

15. OTHER DUTIES OF JUNGHEINRICH

15.1 Upon request by the Customer in writing or text form, Jungheinrich is obliged to support and cooperate in a reasonable manner with 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) within the scope of prior consultations with the supervisory authorities as well as

(d) when the records of Processing activities are drawn up by the Customer.

Even in the event of cooperation or support of the Customer by Jungheinrich, the actions or documentation referred to in (a) - (d) remain under sole responsibility and accountability of the Customer.

Jungheinrich may demand an expense-related remuneration for the support services specified in (a) - (d) on the basis of the hourly rates agreed in the Main Contract.

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 in accordance with the applicable statutory provisions. In all other respects, the liability provisions of the Jungheinrich T&Cs apply.

17. FINAL PROVISIONS

17.1 Amendments to this Agreement and ancillary agreements must be made in writing or by 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 the 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 relating to the obligations relating to the Processing of personal data in the context of the Processing described in **Appendix 2**, **Appendix 3** and **Appendix 4** to this Agreement shall prevail over the Main Contract.

18. LIST OF APPENDICES

The following appendices are an integral part of this Agreement:

- **Appendix 1** : Template letter of accession
- **Appendix 2**: Categories of personal data
- **Appendix 3**: Categories of Data Subjects
- **Appendix 4**: Details of Processing
- **Appendix 5**: Technical and organisational measures
- **Appendix 6**: Sub-processors

Appendix 1

Appendix 1 – Template letter of accession

From: [*name of company to accede to Agreement*]
[Address]

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

[*Date*]

ACCESSION TO THE DATA PROCESSING AGREEMENT FOR DIGITAL JUNGHEINRICH PRODUCTS

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

In accordance with Clause 3.2 of the Agreement, we hereby accede to the Agreement, including all Appendices, under the terms and conditions set out in Clause 3 with effect from *[accession date]*.

For: [*name of acceding company*]

Name: _____

Role: _____

Place, date: _____

Signature: _____

Appendix 2

Appendix 2 – Categories of personal data

The following categories of personal data are processed for the Digital Jungheinrich Products selected by the Customer in the Main Contract:

Categories of personal data	Jungheinrich FMS						
	Starter Kit	Finance Bundle	Access Bundle	Productivity Bundle	Safety Bundle	Safety Bundle Plus	Energy Bundle
Basic personal information	x	x	x	x	x	x	x
Communication data	x	x	x	x	x	x	x
Log data	x	x	x	x	x	x	x
Vehicle user data	x		x	x	x	x	x
Vehicle data	x		x	x	x	x	x
Geolocation							
Medical data					(x)*	(x)*	

Categories of personal data	Jungheinrich FMS						
	Equipment/ Location/ Contracts API	Operating costs API	Operating hours API	Shock management API	Operations API	Employees API	Access management API
Basic personal information						x	x
Communication data	x	x	x	x	x	x	x
Log data	x	x	x	x	x	x	x
Vehicle user data	x		x	x	x	x	x
Vehicle data	x		x	x	x	x	x

The above-mentioned data categories generally include the following data, which may 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, alternative email address, 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, date of issue, expiry date, driver experience level, logon information,

access ID, PIN, external ID, authorisation, hourly rate, certification expiry, licence expiry date, group assignment, driving times, crash 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)

- Geolocation (e.g. WiFi location, GPRS location)

- 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 1.8 of the Agreement. For further information please refer to Appendix 4 Annex A.)

The Digital Jungheinrich Products provided by Jungheinrich are regularly amended and updated to meet new technical and legal requirements. This may result in changes to the categories of personal data Processed in the individual bundles of the Digital Jungheinrich Products. 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.

Appendix 3

Appendix 3 – Categories of Data Subjects

Personal data for the following categories of Data Subjects are processed for the Digital Jungheinrich Products selected by the Customer in the Main Contract:

Categories of Data Subjects	Jungheinrich FMS						
	Starter Kit	Finance Bundle	Access Bundle	Productivity Bundle	Safety Bundle	Safety Bundle Plus	Energy Bundle
Users	x	x	x	x	x	x	x
Drivers			x	x	x	x	x
Signatories of service reports		x					

Categories of Data Subjects	Jungheinrich FMS API							
	Equipment/ Location API	Contracts API	Operating costs API	Operating hours API	Shock management API	Operations API	Employees API	Access management API
Users	x	x	x	x	x	x	x	x
Drivers	x				x	x	x	x

The Digital Jungheinrich Products 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 Digital Jungheinrich Products. An up-to-date 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.

Appendix 4

Appendix 4 – Details of Processing

The Digital Jungheinrich Products offered by Jungheinrich can be ordered with different service packages ("**Bundles**"). The Bundles are selected on the Customer's ~~Cover~~ Main Contract. This **Appendix 4** contains more detailed information on the Processing data for each Digital Jungheinrich Product, and in particular on the type and purpose of the Processing data as well as on the categories of personal data and Data Subjects concerned. Details of the Processing for each Digital Jungheinrich Product can be found in the annexes to this **Appendix 4**. **Appendix 2** contains an overview of the data categories Processed in the respective Bundles, and **Appendix 3** contains an overview of the categories of Data Subjects affected by the Processing within the scope of the respective Bundle.

Annexes to Appendix 4	**Jungheinrich Digital Product**
Annex A	Jungheinrich Fleet Management System ("**Jungheinrich FMS**")
	Starter Kit
	Finance Bundle
	Access Bundle
	Safety Bundle
	Productivity Bundle
	Safety Bundle Plus
	Energy Bundle
Annex B	Jungheinrich FMS Application Programming Interface ("**API**")
	Equipment/ Location / Contracts API
	Operating costs API
	Operating hours API
	Shock management API
	Operations API
	Employees API
	Access management API
No personal data is Processed on behalf of the Customer in the case of the following Digital Jungheinrich Products. Jungheinrich is Controller with regard to the following Digital Jungheinrich Products. The listing is provided as an overview of all Digital Jungheinrich Products.	
Annex C	Call4Service

Appendix 4 Annex A

Annex A – Jungheinrich FMS

Type and purpose of the Processing

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.

Categories of personal data

The categories of personal data affected by the Processing under each Bundle are set out in **Appendix 2**.

Categories of Data Subjects

The categories of Data Subjects affected by the Processing of data under each Bundle are set out in **Appendix 3**.

Jungheinrich FMS Bundles

1. **Starter Kit**

   Type and purpose of the Processing

   The Starter Kit includes an inventory function that is used to digitise warehouses. This provides a platform for the digitisation of the fleet. 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 Kit enables optimization of fleet capacity. This is done on the basis of forecasts at the fleet, vehicle and contract data. The analysis function determines the respective costs per operating hour and presents these over individually selectable periods of time and historical profiles. Invoices are processed for the analysis. These usually contain personal 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.

2. **Finance Bundle**

Type and purpose of the Processing

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.

3. **Access Bundle**

Type and purpose of the Processing

The Access Bundle 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.

4. **Safety Bundle**

Type and purpose of the Processing

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

The shock management function provides data on shocks and offers configurable truckr eactions (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 areused together with the access control. This means that the Access Bundle is already included in the Safety Bundle.

5. **Productivity Bundle**

Type and purpose of the Processing

In addition to the access functionalities, the Productivity Bundle 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.

6. **Safety Bundle Plus**

Type and purpose of the Processing

The Safety Bundle Plus combines the functionalities of the Safety Bundle and the Productivity Bundle. It thus provides data on 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 capacities of the industrial truck fleet and the Customer's fleet. The data for determining the capacity refers to the operating times of the vehicles.

7. Energy Bundle

Types and purpose of the Processing

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.

Data retention periods

The regular retention periods for personal data and the main non-personal data are described below:

Table with regular retention periods of personal data within the JH FMS

Customer data	Retention period	Affected Bundles
Driver names and transponder IDs in Operations reports	6 months	Access Bundle, Productivity Bundle, Safety Bundle (Plus)
Driver names and transponder IDs in Access management	Until end of contract or expiration of licence, respectively manual deletion through customer	Access Bundle, Productivity Bundle, Safety Bundle (Plus)
Names of logged in user in audit logs	18 months	All available Bundles
Driver names and transponder IDs in Pre-Op Check and Quick Check reports	6 months	Safety Bundle (Plus)
Driver names and transponder IDs in Shock report	6 months	Safety Bundle (Plus)
Name and signature of the signatory of Service reports (PDF files)	Maximum of 2 years and 36 days. PDF files are available from 1st of January of the previous year until the current day	Finance Bundle

Table with regular retention periods of non-personal data within the JH FMS

Customer data	Retention period	Explanation of retention period above 5 years	Affected Bundles
Pre-Op Check reports	2 years		Safety Bundle (Plus)
Active checklists	Until the end of the contract or expiry of the licence	Necessary for the provision of the product	Safety Bundle (Plus)
Shock reports	2 years		Access Bundle, Safety Bundle (Plus)
Operations reports	2 years		Access Bundle, Productivity Bundle, Safety Bundle (Plus)
Service reports	Until the end of the contract or expiry of the licence	Necessary for the provision of the product	Finance Bundle
Maintenance service appointments	5 years		Finance Bundle
Customer master data: **Client, equipment, location, tags, licence, locations' business hours, limits**	Until the end of the contract or expiry of the licence	Necessary for the provision of the product	All available Bundles
Productivity Limits: Peak utilization, equipment utilization	Until the end of the contract or expiry of the licence	Necessary for the provision of the product	Productivity Bundle, Safety Bundle (Plus)
Operations for productivity metrics	2 years		Productivity Bundle, Safety Bundle (Plus)
Costs & Operating Hours limits:	Until the end of the contract or expiry of the licence	Necessary for the provision of the product	Finance Bundle

equipment, location, licence, cost value limit on annual costs, meter reading limit on operating hours,			
Technical system backups: log files, backup data	6 months		All available Bundles
Operating hours	Until the end of the contract or expiry of the licence	Necessary for the provision of the product / Contractual requirement	All available Bundles
Data from sales contracts, rental contracts, service contracts	Until the end of the contract	Necessary for the provision of the product / Contractual requirement	Starter Kit, All available Bundles
Cost information **(incl. invoices/invoice Items and user-created invoices)**	Until the end of the contract or expiry of the licence	Necessary for the provision of the product	Finance Bundle
Battery- and charging related data	2 years		Energy Bundle

Optionally applies if there is a contractual agreement on the use of the FMS API (interface):

Customer data	Retention period	Explanation of retention period above 5 years	Affected API categories
FMS API base data: customer, location, equipments, tags (attributes), licenses	Until the end of the contract or expiry of the licence	Necessary for the provision of the API	All available API categories
API key Management (incl. audit logs)	Until the expiry of the licence	Necessary for the provision of the API	All available API categories

Appendix 4 Annex B

Annex B – Jungheinrich FMS API

Type and purpose of the Processing

Upon instruction of the Customer, Jungheinrich provides personal data Processed on behalf of the Customer in the course of providing the Jungheinrich FMS as described in Annex A to Appendix 4 to the Customer via the Jungheinrich FMS API.

The provision of personal data via the Jungheinrich FMS API is divided into different API categories that are purchased individually by the Customer and have different requirements with regard to the corresponding Bundles that are a pre-requisite for the respective API. The respective purposes as well as the data Processed in each case are described below according to the each API category.

Categories of personal data

The categories of personal data affected by the Processing under each API category are set out in **Appendix 2**.

Categories of Data Subjects

The categories of Data Subjects affected by the Processing of data under each API category are set out in **Appendix 3**.

Jungheinrich FMS API categories

1. **Equipment/ Location / Contracts API**

   Type and purpose of the processing

   Equipment API retrieves data about all vehicles currently present at the requested location. Vehicle is a piece of fleet, which currently assigned to a location. Data set consists of a serial number, segment, construction year, and other fields that provide detailed information about the specific equipment.

   Location API retrieves data about locations with information such as address, postal code, etc.

   Contracts API retrieves contract information for vehicles at the specified location: contract type, contract number, start and end date, agreed number of operating hours, rental types and other contract related information. One vehicle can have multiple contracts.

   To be able to get an access to data from a specific location and to retrieve data the Customer must use an API key, which is created for the Customer. API key and IP address can be tracked by Jungheinrich.

2. **Operating costs API**

   Type and purpose of the processing

   Operating costs API retrieves costs for a vehicle in the specified location in the specified time range. The returned data block is a list of entries in which every entry is related to specific vehicle.

   To be able to get an access to data from a specific location and to retrieve data the Customer must use an API key, which is created for the Customer. API key and IP address can be tracked by Jungheinrich.

3. **Operating hours API**

Type and purpose of the processing

Operating hours API retrieves all the operating hour measurements sent from a vehicle in a given location with the location_id parameter and in certain time frames using the from and to query parameters. An operating hour measurement is a recording of the current operational hours of a given vehicle, measured in hours, including a timestamp when then measurement was recorded. Beside that the measurements for all the vehicle that is or was assigned to the given location and was recorded between the given from and to query parameters can be retrieved. To be able to get an access to data from a specific location and to retrieve data the Customer must use an API key, which is created for the Customer. API key and IP address can be tracked by Jungheinrich.

4. Shock management API

Type and purpose of the processing

Shock management API retrieves all the relevant telematic data from a shock event for a given location using the location_id parameter. A shock event is sent from a vehicle which experiences a sharp force from hitting another object or a bump on the ground, for example. The intensity is recorded in two dimensions, as well as the consequence which indicates if the vehicle can continue driving, has enabled crawl speed or in severe cases, has automatically shut down.

To be able to get an access to data from a specific location and to retrieve data the Customer must use an API key, which is created for the Customer. API key, IP address and configuration changes in the management portal can be tracked by Jungheinrich.

Shock events are enriched with additional information (e.g. time, vehicle number, transponder ID) in order to identify unsafe operation patterns at an early stage and to avoid consequential damage or safety risks for employees. The employees who carry out the respective departure on a vehicle can be identified by name when combining data provided in Shock management API and Employees API.

5. Operations API

Operations API retrieves data such as start and end date and time of operation, operation duration, switch-on and -off times of the vehicle etc. Operations API data provide the users with a holistic overview of the use of the fleet and allow to detect possible misuse. Usage data are enriched with additional information (e.g. time, vehicle number, the type of logout, multi-login, transponder ID) in order to identify cases of misuse at an early stage and to avoid consequential damage or safety risks for employees as well as not optimal usage of the vehicle. The employees who carry out the respective departure on a vehicle can be identified by name when combining data provided in Operations API and Employees API.

To be able to get an access to data from a specific location and to retrieve data the Customer must use an API key, which is created for the Customer. API key, IP address and date and time of logon and logoff of a driver to a specific vehicle can be tracked by Jungheinrich.

6. Employees API

Employees API retrieves employee's data at a given location: employee ID, first name, last name, transponder ID, role etc.

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.

To be able to get an access to data from a specific location and to retrieve data the Customer must use an API key, which is created for the Customer. API key, IP address can be tracked by Jungheinrich.

7. Access management API

Type and purpose of the processing

Access management API retrieves the access configuration data for a given vehicle using the vehicle_id parameter at a given location using the location_id parameter. A vehicle access configuration offers relevant vehicle configuration (e.g. timeout values) and if access is enabled/disabled. It also includes the information, when a configuration was sent to the vehicle and when it was acknowledged by the vehicle. There is a default configuration that can be overwritten e.g. by sending an API post requests. An updated configuration will be acknowledged by the truck.

Access management API is used to configure an access to a vehicle and to protect the fleet from unauthorised use without usage of the Jungheinrich FMS user interface. 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.

Beside that this API allows Customer to create, retrieve, update and delete employees at a given location. To be able to get an access to data from a specific location and to retrieve data the Customer must use an API key, which is created for the Customer. API key, IP address can be tracked by Jungheinrich.

Annex C – Call4Service

No personal data is Processed on behalf of the Customer.

Information on Processing can be found in the product privacy policy.

In the event that subsequent changes to the product result in Jungheinrich being a Processor in accordance with data protection regulations, this **Hiba! A hivatkozási forrás nem található.C** to **Appendix 4** will be replaced accordingly.

Appendix 5 – 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 Processing, and amends the TOMs as necessary to ensure a continuously high level of protection.

The listing concerns the entirety of Digital Jungheinrich Products. The TOMs to be applied may vary depending on the product.

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
- 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 **Appendix 5** shall also apply, as far as applicable, in the case of remote access to the personal data.

Appendix 6

Appendix 6 – Sub-processors

For the Processing of personal data on behalf of the Customer, Jungheinrich uses the services of third parties who Process personal data on its behalf ("**Sub-processors**"). These are listed in the overview below.

Sub-processors (Name, legal form, registered office of the company)	**Type of service provided**	**Digital Jungheinrich Product**	**Processing location** (place of Processing)
Jungheinrich Digital Solutions AG & Co.KG Sachsenstr. 20, 20097 Hamburg, Germany	• Development • Maintenance & Support • IT Administration	• Jungheinrich FMS	
Jungheinrich Digital Solutions S.L. Calle Gran Via nº 30 - Planta 7, 28013 Madrid, Spain	• Development • Maintenance & Support • IT Administration	• Jungheinrich FMS	
Jungheinrich AG Information Technology Friedrich Ebert Damm 129, 22047 Hamburg, Germany	• Service Hosting	• Jungheinrich FMS	Server locations: • Hamburg, Germany (Jungheinrich AG IT) • Frankfurt, Germany (Equinix Germany GmbH)
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg	• Service Hosting	• Jungheinrich FMS	Server locations: • Frankfurt, Germany • Dublin, Ireland • Paris, France • Stockholm, Sweden • Milan, Italy
Jungheinrich Business Services Romania S.R.L. Brasov, Saturn Blvd. No. 51, 5th floor, 105440 Brasov county, Romania	• IT Administration • Support	• Jungheinrich FMS	
Jungheinrich Business Services Croatia d.o.o. Slavonska avenija 1C 10000 Zagreb, Croatia	• Development • Maintenance & Support • IT Administration	• Jungheinrich FMS	
Jungheinrich Svenska AB Starrvägen 16 232 61 Arlöv, Sweden	• Development • Maintenance & Support • IT Administration	• Jungheinrich FMS	
Splunk Services Germany GmbH Salvatorplatz 3, 80333 Munich, Germany	• Storage and processing of log data	• Jungheinrich FMS	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)	• Jungheinrich FMS	Server locations: • Germany West Central (Frankfurt) • West Europe (Netherlands) • North Europe (Ireland)
Device Insight GmbH Willy-Brandt-Platz 6, 81829 Munich, Germany	• IoT service (provision of IoT interface)	• Jungheinrich FMS	
ClickHouse, Inc. 650 Castro St., Suite 120 #92426, Mountain View CA 94041, USA	• Cloud-based data analysis and evaluation	• Jungheinrich FMS	Server location: • Frankfurt, Germany