Appendix to the existing contractual relationship

for the Kubernetes extension HariKube

between

Company

Address

Location

hereinafter referred to as the CLIENT
and the

inspirNation Bt.

HU 2161 Csomád

Levente utca 14

hereinafter referred to as the CONTRACTOR,

Regarding the contract: Contract number

Preamble

This addendum specifies the obligations of the contracting parties arising from the contractual relationship for the provision and use of the Kubernetes software extension “HariKube.” It applies to the parameters related to the contractual relationship for the provision of IT services required to support and maintain the product or service.

This agreement shall remain valid until it is replaced by a revised agreement mutually approved by the stakeholders or until the underlying contractual relationship expires.

§ 1 Subject matter, duration, and specification of the IT service

(1) The subject matter and duration of the contract are determined by the above-mentioned contractual relationship. The term of this annex is based on the term of the contractual relationship, unless further obligations arise from the provisions of this annex.

(2) Type of IT service:

- Hosting the contractor's own software “HariKube” for the client using the clients own IT infrastructure.
- Providing secure access to the services for the client.
- Providing the latest Harikube releases for download.

To implement these services, the contractor uses its current technical and organizational measures (TOMs) in accordance with the GDPR.

§ 2 Availability

(1) The contractor shall endeavor to achieve a minimum availability of 98.5% per annum for the hosted software.

(2) Harikube is available to the customer for download around the clock, seven days a week, subject to the following restrictions:

- Disruptions due to force majeure.
- Disruptions caused by components outside the contractor's area of responsibility.
- Misuse of the software by the client.
- Downtime due to disruptions.
- Downtime due to defined maintenance by the contractor.
- Downtime due to data backups.

§ 3 Support

(1) In the event of disruptions to the IT services provided by the contractor in accordance with §1, the client shall have access to a support hotline at least from Monday to Thursday from 9:00 a.m. to 4:00 p.m. CET and on Friday from 9:00 a.m. to 12:00 p.m. CET (excluding public holidays).

(2) Faults can be reported to the contractor as follows:

- Contact: HK-Support
- Email: support@inspirnation.eu

§ 4 Maintenance

(1) The maintenance work on hardware, software, network, and security components necessary to maintain the IT infrastructure will preferably be carried out between 5:00 p.m. and midnight CET on the third Tuesday of each month.

§ 5 Incident management

(1) The faults reported by the client are recorded and processed in the following manner:

	Step	*Description*
1.	**Reporting**	The client should provide as much information as possible when reporting the fault, in particular: Specification of the fault, in particular the time of the fault, application environment and situation, frequency of the problem and error messages. If appropriate, screen shots can be used to document the error.
2.	**Registration**	The client's report is registered, and receipt of the report is confirmed.
3.	**Determining priority**	The priority of the malfunction is determined, and the necessary departments of the contractor are informed.
4.	**Diagnosis**	Analysis of the malfunction and its causes (e.g., by reproducing the malfunction in different environments). Consultation with the client for necessary information.
5.	**Searching for and, if necessary, implemen-ting a solution**	A solution is sought for the malfunction and, if necessary, implemented in the system environment.
6.	**Feedback**	Once the issue has been resolved, the customer will be informed that a new Harikube version has been deployed.

(2) The faults reported by the client are divided into 3 priority levels.

Priority	*Description*	*Processing*
1 ***Critical Incident***	One or more of the following cases apply: ● Production data/information has been destroyed or lost. ● One or more components of the IT infrastructure are not functioning, and the disruptions are causing serious interruptions. ● Security vulnerabilities in the overall system	The disruption will be handled as a priority by all relevant departments. All necessary resources (redundancies, backups) will be used to restore operations as quickly as possible.
2 ***Fault to be tolerated temporarily***	The malfunction has no direct critical consequences, but productivity is hampered by the limited functionality of the system.	The fault will be analyzed and processed by the responsible department. Depending on the severity of the fault, it will be rectified during the maintenance period, with an update, or within a reasonable period of time.

3 ***Improvement***	The fault does not fall into category 1 or 2, but the customer wants an extension, adjustment, or a change.	The reported “improvements” are analyzed as part of the software update service. If these have a positive effect on the overall system, they are integrated after approval by the contractor's management. Larger, customer-specific, or special changes are regulated via separate contractual relationships.

§ 6 Privacy and security

(1) The data protection obligations are set out in the annex to the existing contractual relationship regarding order processing within the meaning of the General Data Protection Regulation (GDPR).

(2) The security of the IT infrastructure and customer-specific data is documented in the “Technical and Organizational Measures (TOM),” which are updated annually. The measures documented therein also apply explicitly to the contractual relationship.

(3) The technical and organizational measures that are implemented in addition to the measures mentioned in 2 are as follows:

- Separate administrators and users manage access to the IT environment.
- Use of a backup server with enhanced security mechanisms.
- Backup hard drives are encrypted three times with a cryptographic key.
- Securing web access for the hosted software via HTTPS with TLS version 1.2 encryption.
- Firewall with deep packet inspection (DPI), intrusion detection system (IDS), and central endpoint monitoring.
- Logging of data access to exclude external data.
- Regular separate security updates.
- Services related to HariKube are provided within the EU.

§ 7 Remuneration

(1) Remuneration for services shall be based on the payment agreements specified in the contract.

§9 Severability clause and written form requirement

(1) Should individually parts of this annex be invalid, this shall not affect the validity of the remainder of the annex. The contracting parties shall agree on a provision to replace the invalid or incomplete provision which comes closest to the economic or legal purpose of the contract and the intentions of the contracting parties in a manner permitted by law.

(2) Amendments and additions to this Annex and all its components, including any assurances given by the Contractor, require a written agreement, which may also be in electronic format (text form), and an express reference to the fact that this is an amendment or addition to these terms and conditions. This also applies to any waiver of this formal requirement.

(3) German law applies, and the place of jurisdiction is Hamburg.
Translations for this purpose are treated as separate services if necessary.

§10 Attachments

(1) The following annexes form an integral part of this annex.

- GDPR annex to the existing contractual relationship
- Checklist of technical and organizational measures (TOMs) in accordance with the GDPR

Csomád,

Signature Client

Signature Contractor

Annex

Technical and organizational measures (TOMs) in accordance with the GDPR

- All data is exchanged exclusively in a secure manner (SSL/TLS).
- Authentication is required for access.
- Additional user-specific authentication is required to access the ERP software in which the data is stored.
- Documentation is available specifying WHO is permitted to access WHICH personal data or systems.
- Before accessing the data, the employees concerned receive the data protection declaration, the information security policy, a confidentiality agreement, and the IT and telecommunications policy, which they must read and sign. In addition, they receive documented initial training.
- The ERP data is backed up daily in physically separate buildings without electrical connections.
- A firewall concept is in place.
- A system with measures for detecting, preventing, and removing malware.
- All documentation is based on ISO 27001 ff.
- Emergency response and BCM are handled by the internal IT department.
- Access to company buildings is restricted to authorized people only.
- Visitors must register and are accompanied by staff at all times during their stay.
- Employees involved in the processing of personal data have been instructed on their obligation to maintain confidentiality and data secrecy.
- After completion of an order, the data is deleted in accordance with legal requirements.
- Rights to enter, modify, and delete data are granted on the basis of an authorization concept.
- Traceability of data entry, modification, and deletion through individual usernames.
- Use of an internal information security officer (CISO).