

GENERAL TERMS FOR THE USE OF IT SOLUTIONS AND PROVISION OF IT SERVICES

1. GENERAL PROVISIONS

These General Terms for the Use of IT Solutions and Provision of IT Services (hereinafter: the **General Terms**) govern the mutual rights and obligations of the company **SPAN d.d., Koturaška cesta 47, 10 000 Zagreb, Croatia, company ID number (OIB): 19680551758** (hereinafter: the **Provider**) and the User in connection with the delivery, maintenance and use of IT Solutions and the provision of IT Services defined in Article 3 of these General Terms (hereinafter collectively: the **IT Solutions and Services**).

These General Terms apply exclusively to the provision and use of the IT Solutions and Services within the European Economic Area (EEA). The User agrees to use the IT Solutions and Services in accordance with this territorial restriction.

For the purposes of these General Terms, the User may be a legal entity or a natural person carrying out a registered business activity who has entered into an agreement with the Provider for the delivery of IT Solutions and provision of IT Services (hereinafter: the **Master Agreement**).

These General Terms form an integral part of each Master Agreement and apply to all offers, purchase orders, deliveries, and use of the IT Solutions and Services, unless otherwise expressly agreed in the Master Agreement or in another written document signed by the Contracting Parties.

2. DEFINITIONS

2.1. The following definitions apply for the purposes of these General Terms:

2.1. “User” means an entity that accepts these General Terms for the purpose of using the IT Solutions and Services for its business purposes. The entity may only be a person carrying out a business activity (such as a legal entity, sole proprietor, self-employed person or similar entity).

2.2. “Offer” means any proposal made by the Provider to the User to enter into an agreement that contains the essential elements of the proposed transaction, (including, but not limited to, a description of the products, services or licenses, the price or the method for determining the price, and other relevant terms), regardless of its name, form or method of delivery. An Offer includes, in particular, the presentation of products, services or licenses on the Provider’s platform (including through a user interface, website or application), if such presentation enables the User to place an order directly or enter into an agreement. An Offer may be made or accepted in writing or electronically, including by email, through online forms, a user interface or other means of electronic communication, or by conduct from which the intent to enter into an agreement can be reliably established, unless otherwise provided in these General Terms. An Offer may not be made or accepted orally. Unless expressly stated otherwise, the Offer binds the Provider for the period specified in the Offer or otherwise for a reasonable period from the date on which it is sent or published.

2.3. “Purchase Order” means an expression of the User’s intent addressed to the Provider whereby, based on an Offer or other relevant presentation of products,

services or licenses, the User orders specific products, services or licenses and expresses its intent to enter into an agreement under the terms set out in the Offer or these General Terms. A Purchase Order may be delivered in writing or electronically, including by email, through online forms, a user interface, the Provider's platform or other means of electronic communication, or by conduct that unequivocally indicates the User's intent to place an order, unless otherwise provided in these General Terms. Unless expressly stated otherwise, by delivering a Purchase Order, the User is deemed to have acknowledged the Offer and these General Terms and accepted them in full.

- 2.4. "Written Form"** means any form of communication by which the content of a statement of intent can be permanently or temporarily recorded and reproduced, regardless of the medium or technical means through which it is transmitted, and which enables the identification of the sender and the content of the statement. Written form includes, in particular, communication by mail, email, online forms, a user interface, information systems or other means of electronic communication. Oral communication does not constitute written form for the purposes of these General Terms.
- 2.5. "Authorized Contact Person"** means a natural person authorized by the User to place orders, make changes, upgrade, cancel and renew subscriptions, receive notices regarding updates to the Master Agreement and the General Terms, and communicate with the Provider regarding all matters related to finances and billing for the services.
- 2.6. "Authorized Technical Person"** means a natural person authorized by the User to report technical issues and/or submit requests related to the IT Solutions and Services provided.
- 2.7. "Authorized Span.Zone Platform Administrator"** means a natural person authorized by the User to administer, order and manage user accounts on the Span.Zone platform.
- 2.8. "Working Hours"** means the period from Monday to Friday from 09:00 to 16:00 local time (CET). Overtime work applies from 16:00 to 09:00, whereby the period from 22:00 is considered night work. Work on Saturdays, Sundays and Croatian public holidays is considered overtime work.
- 2.9. "Tenant"** means a logically separate and isolated cloud environment within the infrastructure of the technology solutions provider that is assigned to and represents a single organization (User) and serves as the central unit for managing user accounts, identities, licenses, security settings, and the use of the associated cloud services.
- 2.10. "Tenant Ownership"** means the legal and operational right of an organization to establish and retain full control over one or more associated Tenants, including, but not limited to, the management of user accounts, identities, data, licenses, and security settings, as well as access to and use of cloud services.
- 2.11. "Affiliate"** means any legal entity that directly or indirectly controls a Contracting Party, is controlled by a Contracting Party, or is under common control with a Contracting Party, where control is deemed to exist if such legal entity directly or indirectly holds more than 50% (fifty percent) of the voting securities or otherwise has the authority to direct the management and business decisions of the relevant legal entity.
- 2.12. "Ticket"** means a digital record of communication between the User and the Provider related to the provision of support and maintenance services that,

depending on the nature of the request, may be classified as an Incident, Problem, Change Request or Request for Information.

- 2.13. “Incident”** means an unwanted event that causes or may cause degradation of system performance or system unavailability.
- 2.14. “Major Incident”** means a type of Incident that has a very high impact on a business service, affects all users of the business service, and requires additional resources to be engaged and emergency communication channels to be activated for its resolution.
- 2.15. “Workaround”** means a workaround solution that may be applied to improve performance or restore system availability.
- 2.16. “Problem”** means the root cause of one or more Incidents, the management of which is carried out with the aim of permanently eliminating the cause and preventing the recurrence of Incidents. Problem Management may be reactive (following the occurrence of Major Incidents) or proactive, based on system monitoring, experience and information provided by the manufacturer.
- 2.17. “Change Request (CR)”** means a request made by the User to the Provider to perform changes that do not affect the operation of the relevant system or the manner in which the relevant system is currently used. Such changes may be requested by an authorized representative of the User.
- 2.18. “Request for Information (RFI)”** means a request made by the User to the Provider for information about the operation of the relevant services, the scope of the services provided, reports and similar matters. It does not include training, the development of technical solutions, consulting and/or project tasks.
- 2.19. “Standard Changes (Service Request)”** means changes that do not affect the operation of the relevant system or the manner in which the relevant system is currently used.
- 2.20. “Major Change”** means changes that alter the manner in which the relevant system operates or affect its operation.
- 2.21. “Emergency Change”** means a specific type of change for which it is critical that the change be implemented as soon as possible. Failure to implement the change could have a very significant impact on the User’s business operations in connection with the services provided by Span. An Emergency Change is performed exclusively during the resolution of a Priority 1 or Priority 2 Incident.
- 2.22. “SLA (Service Level Agreement)”** means the terms and methods of providing support and maintenance services provided by the Provider to the User.
- 2.23. “Service Desk”** means the single point of contact for the User as part of the provision of support and maintenance services.
- 2.24. “Response Time”** means the time elapsed from the moment an Incident is reported or, in the case of proactive monitoring, detected, until the User is notified by non-automated means that the Incident has been received or detected.
- 2.25. “Resolution Time”** means the time elapsed from the moment a Ticket is logged until the moment it is determined that the effects caused by the Incident are no longer evident or no longer affect operation. For a CR and a RFI, the Resolution Time ends when the request has been fulfilled or the inquiry has been answered, respectively.

- 2.26. “Remote Access”** means access to an IT system or its components without physical presence (VPN).
- 2.27. “OS (Operating System)”** means the basic software that manages hardware resources and enables applications to run.
- 2.28. “SLA Standard (8x5)”** means a support model provided during Working Hours.
- 2.29. “SLA Standard+ (24x7 for Sev.1)”** means a support model provided every day from 00:00 to 24:00 for all Priority 1 Incidents, while response times for all other Incidents and requests apply only during Working Hours.
- 2.30. “SLA Gold (24x7)”** means a support model provided every day from 00:00 to 24:00 for all Incidents and requests of the User.
- 2.31. “Technical Support”** means services provided by the Provider to users in connection with the use of the Span.Zone platform, including assistance with the use of functionalities, management of user accounts and Tenants, and support related to products and services. Technical Support may be provided free of charge or for a fee, whereby chargeable support is provided and billed in accordance with the applicable Offer provided at the User’s request.

3. IT SOLUTIONS AND SERVICES

3.1. Types of IT Solutions and Services

The IT Solutions and Services provided by the Provider to Users include:

(a) Microsoft products and services:

- subscriptions to Microsoft online services;
- Microsoft software subscriptions;
- Azure:
 - Azure consumption;
 - Azure Reservations;
 - Azure Savings;
 - Azure Marketplace;
- Microsoft perpetual licenses.

(b) Google products and services:

- Google product subscriptions (Google Workspace);
- Google Cloud Platform (GCP):
 - On-demand Pay-as-you-go;
 - Committed use discount (GCP);
 - Sustained use discount (GCP);
- Cloud Identity — identity and access licenses (IAM);
- Chrome Enterprise / ChromeOS licenses.

(c) Support and maintenance:

- Microsoft 365 support.

The specific scope, quantity and duration of individual IT Solutions and Services are defined in the Master Agreement.

3.2. Third-Party Products and Related Services Provided by the Provider

The scope, content, functionalities, quality, availability, duration of user rights and terms of use of third-party products and services, including, but not limited to, Microsoft and Google products and services (hereinafter: the “Third-Party Products”), are determined exclusively by their respective issuers or service providers (hereinafter: the “Manufacturers”) and are governed by their applicable terms of use, policies, licensing terms, SLAs and technical documentation.

Without prejudice to the foregoing, the scope, quality and duration of use of Microsoft products and services are defined by Microsoft in the applicable Microsoft Customer Agreement (hereinafter: the “Microsoft Customer Agreement”) and the related documentation. The Provider has no influence over the development, content or terms of provision of Microsoft products and services, and such products and services are provided to the User exclusively to the extent, quality and for the duration specified in the Microsoft Customer Agreement, without any modifications or additions by the Provider. In the event of any inconsistency between the provisions of the Microsoft Customer Agreement and the provisions of these General Terms or the Offer, the provisions of the Microsoft Customer Agreement shall apply to the extent relating to Microsoft products and services.

The Manufacturers have the right to unilaterally change, supplement or discontinue their products and services at any time, including their functionality, availability, technical specifications, security features and licensing models, in accordance with their own business policies.

The Provider has no influence over the development, content, modifications, availability, continuity of provision or terms of use of the Third-Party Products and, in this respect, makes no warranties and assumes no liability for the following, including, but not limited to:

- availability or uninterrupted operation;
- changes to functionality or discontinuation of individual features;
- changes to licensing models or prices;
- security or technical changes;
- interoperability with other systems.

The Third-Party Products are provided to the User on an “as is” and “as available” basis, in accordance with the terms determined by the Manufacturers.

The User must use the Third-Party Products in accordance with the applicable terms, policies and licensing terms of the respective Manufacturer and is responsible for any breach thereof.

The Provider is responsible solely for its own services provided to the User in connection with the Third-Party Products (including administration, implementation, maintenance, support and billing), and only to the extent expressly agreed in the Offer or the Master Agreement, but is not responsible for the operation or availability of the Third-Party Products provided.

The support and maintenance services provided by the Provider in connection with the Third-Party Products are subject to the capabilities and limitations imposed by the Manufacturers, including the availability of administrative tools, access (e.g., tenant or delegated access), documentation and Manufacturer support, and the Provider is not responsible for any inability or limitations in providing such services arising from the actions or limitations of the Manufacturers.

3.3. Microsoft Products and Services

The Provider supplies Microsoft products and services as an authorized Cloud Solution Provider (CSP) partner of Microsoft Ireland Operations Limited (hereinafter: Microsoft), exclusively through the CSP program.

The Provider is authorized to:

- offer and distribute Microsoft products and services covered by these General Terms;
- receive settlement of Microsoft's claims from the User;
- provide expert technical assistance in connection with the use of Microsoft products and services.

For the use of Microsoft products and services, the User is required to accept the Microsoft Customer Agreement, which is deemed to be a separate agreement entered into between Microsoft and the User upon the delivery of Microsoft products and services and which applies directly between the User and Microsoft. The Provider participates in this relationship as Microsoft's contractual partner in the distribution chain, without having any influence over the content of the aforementioned agreement.

The User is required to ensure acceptance of the Microsoft Customer Agreement during the period from the execution of the Master Agreement until the delivery of Microsoft products and services.

The Microsoft Customer Agreement is deemed to have been duly accepted by the User no later than upon the delivery or activation of the Microsoft products or services and may, in particular, be accepted by:

- signing the Master Agreement;
- accepting an Offer that contains or refers to the Microsoft Customer Agreement;
- issuing a Purchase Order; or
- accepting it through the Microsoft admin portal (available at the following link: [Microsoft 365 admin center](#)) by a person with global administrator rights in the system (e.g., status "Customer acceptance through Microsoft: PROVIDED"), depending on which of the above events occurs first.

Microsoft Licensing Documents are available at the following link: [Licensing Documents](#).

If the Microsoft Customer Agreement has already been entered into between the User and Microsoft, it remains in force and applies to all existing and future Microsoft products and services covered by the Master Agreement.

The User represents and warrants, under full material and legal liability, that it is the lawful owner and/or authorized holder of the Tenant to which the Microsoft products and services relate and that it is authorized to accept the Microsoft Customer Agreement on its own behalf and/or on behalf of the legal entity it represents.

The User confirms that it is authorized to accept and that it accepts the Microsoft Customer Agreement on its own behalf and/or on behalf of the entity it represents, and the Provider is not liable for any inaccuracy or untruthfulness of the User's statements or for any consequences that may arise from the unauthorized use of or dealings with the relevant Tenant.

The Microsoft Customer Agreement forms an integral part of the contractual framework governing the use of Microsoft products and services and applies directly between the User and Microsoft.

The Microsoft Customer Agreement also forms an integral part of these General Terms. In the event of any inconsistency, contradiction or differing interpretation between the Microsoft Customer Agreement and these General Terms, the provisions of the Microsoft Customer Agreement shall prevail and take precedence.

3.3.1. Transfer of MS Products and Services

In the event of a transfer of a subscription from another Microsoft partner to the Provider, the Provider does not assume responsibility for the User's obligations to the previous partner.

The Provider will accept the User as a partner only upon receipt of valid confirmation that all obligations to the previous partner have been fully settled, irrespective of the execution of the Master Agreement or acceptance of these General Terms.

In the event of a transfer of a subscription from the Provider to another partner, the User's obligations to the Provider cease on the date on which the transfer is completed, provided that all due invoices have been paid in full.

The Provider reserves the right to charge for all services provided up to the date of the transfer, including related costs, and is not responsible for the further provision of services after the date of the transfer.

3.3.2. Tenant Naming

The User agrees that the Tenant may be named at the User's discretion and accepts that the Tenant name may, but need not, contain the User's name or another identifier selected at the time the Tenant is created.

The naming of the Tenant has no effect on ownership of the Tenant or on the User's rights and obligations arising from the use of Microsoft cloud services.

3.3.3. Changes Concerning the User

In the event of a change in the User's name, legal form, status or ownership structure, the User is required to notify the Provider of such change in a timely manner and, where necessary, ensure the appropriate modification or migration of the Tenant. All costs, as well as the technical and contractual consequences of such changes, are borne solely by the User.

The Provider is not liable for any consequences arising from the User's failure to notify the Provider of the aforementioned changes in a timely or accurate manner.

3.3.4. Responsibility in the Event of an Audit

In the event of an audit or compliance review conducted by Microsoft or a third party authorized by Microsoft, the User bears full responsibility for the lawful and contractually compliant use of licenses, services and access rights within its own Tenant.

3.3.5. Extended Service Term

Upon renewal of a subscription, the User may expressly request the application of the Extended Service Term (EST) service, in accordance with Microsoft's applicable rules and terms. The service constitutes an additional type of subscription and applies solely upon the User's prior request.

The terms, duration and price of the service are set out in a separate Offer issued by the Provider, in accordance with the applicable price list and the Manufacturer's rules.

3.4. Support and Maintenance

Support and maintenance services include troubleshooting as required or at the User's request.

The support and maintenance services provided by the Provider to the User are described in detail in these General Terms and the applicable Offer under the Master Agreement and are performed in accordance with the agreed terms, timeframes and SLA parameters, if such parameters have been agreed.

The Provider will notify the User without undue delay of any significant changes that may affect the use of its system and that are relevant to the performance of the agreed services.

Support and maintenance services are provided through Remote Access from the Provider's location, unless otherwise agreed.

A prerequisite for the provision of support and maintenance services in connection with Microsoft 365 is that the User grants the Provider appropriate access through a delegated administrator.

3.4.1. Scope of Microsoft 365 Support Services

The support service provided at the User's request includes:

- free support, including L1 and L2 support levels:
 - management of license provisioning and renewal;
 - verification of the operational status of Microsoft online services;
- chargeable technical assistance and support for Microsoft 365, including L1, L2 and L3 support levels:
 - installation and configuration of Microsoft 365 tools;
 - troubleshooting issues related to the use of Microsoft 365 tools;
 - resolution of incidents related to Microsoft 365 services;
 - modifications and changes to Microsoft 365 and its services;
 - creation or deletion of user accounts;
 - creation of shared mailboxes;
 - administration of users and groups;
 - administration of SharePoint, Exchange, Microsoft Teams and other services;
- the ability to report issues and requests to the Operations Center 24x7;
 - the Standard support level applies to the services specified above.
- requests are handled:
 - through the Microsoft 365 admin center;
 - by remote access to a computer at the User's request.

3.4.2. Out-of-Scope Services

Unless otherwise stated, all activities that are not within the scope are outside the scope of the Technical Support services.

For requests that fall outside the scope of the Technical Support services provided, the Provider will, if it is able to fulfil the request, conduct an evaluation and submit an Offer specifying the timeframes for fulfilling the User's request. The Provider will proceed with fulfilling the request only after the Offer has been accepted, in accordance with the terms of the Offer.

All data stored within the system delivered by Span or managed by the Provider are owned by the User, and it is the User's responsibility to ensure data backup in production systems. If the Provider is responsible for the data restoration process from backup, the data will be restored "as-is". During data retrieval from backup, the Provider will attempt to restore the data to its original state; however, it is the User's responsibility to ensure that such data can be read by business processes.

If the installation of application or security patches falls within the scope of the service provided by the Provider, such installation includes only the IT operational activity of installation. In accordance with the manufacturer's recommendations, such installation does not include any service related to Cyber Security Operations, Security Analysis, Security Incident Response or other services.

The User is required to obtain all necessary licenses for the performance of the service in accordance with the agreed terms.

3.4.3. IT Support

The Provider's support and maintenance service is organized in accordance with the standards (ISO 20000, ISO 27000, ISO 9000) as well as industry best practices (ITIL).

In the event of performance degradation or a complete interruption of the relevant service, the Provider will proceed with troubleshooting and restoring the normal functionality of the service through three levels of support:

- **First-level support (L1):** acceptance and classification of incidents and undertaking all necessary actions to restore normal service functionality within the shortest possible time. If first-level support is unable to resolve the incident within the agreed timeframe, the incident is escalated to second-level support.
- **Second-level support (L2):** in cases where greater expertise is required to resolve the incident, second-level support takes over its resolution.

If second-level support is unable to resolve the incident within the agreed timeframe, the incident is escalated to the next (higher) support level.

- **Third-level support (L3):** represents the highest level of expertise required to establish and maintain normal service functionality and may be provided by highly certified experts in various technologies at the Provider's disposal or directly by the vendor of the relevant technology/solution.

The purpose of this organization is to ensure the availability of the Provider's expertise to the User, with the aim of restoring normal functionality of the relevant services within the shortest possible time.

3.4.3.1. Span Service Desk

For the purpose of providing support and maintenance services in accordance with the User's requirements and expectations, the Provider will ensure a single point of contact – the Service Desk.

The Service Desk will record all communication with the User in the form of a single digital record, referred to as a ticket.

There are three types of tickets:

Incident	An Incident is opened in the event of performance degradation or complete unavailability of the relevant services. An Incident may be reported by the User or opened automatically through the monitoring system, if established.
Change Request (CR)	A Change Request is opened at the request of an authorized representative of the User when there is a need to perform a Standard Change. The list of pre-approved Standard Changes is provided in the “Request Management” section.
Request for Information (RFI)	A Request for Information is opened at the User’s request when the User requires information about the operation of the relevant services, the scope of the service provided, reports and similar matters. It does not include training, development of technical solutions, consulting and/or project tasks.

3.4.3.2. Communication Methods and Contact Details

The User may contact the Span Service Desk through the following communication channels:

- **Phone:** +385 (1) 6690 222
- **E-mail:** support@span.eu
- **Web portal:** <https://span.support>

Span Service Desk Working Hours

The Span Service Desk is available according to the following schedule:

- **on business days:**
 - from 00:00 to 24:00 for Priority 1 incidents,
 - from 09:00 to 16:00 for all other requests and incidents.
- **on weekends:**
 - from 00:00 to 24:00 exclusively for Priority 1 incidents.
- **on public holidays:**
 - from 00:00 to 24:00 exclusively for Priority 1 incidents.

All requests and incidents are received and processed through the above communication channels, with the priority determined in accordance with the agreed service levels (SLA).

3.4.3.3. Technical Support – SLA Standard

- The service is designed so that Users can access the Provider’s technical experts (L1, L2, L3) when needed.
- Incident/problem management.
- Request fulfilment (changes and requests for information).

3.4.3.4. Incident and Problem Management

In the event of Incidents, the User shall contact the Span Service Desk and report the issue with as much detailed information as possible.

The Span Service Desk shall record the report in the form of an Incident Ticket and proceed with its resolution in accordance with the response times specified for the relevant service.

The priority for resolving an Incident is determined in accordance with the table of response times specified for the relevant service.

The purpose of the service is to restore the relevant service to operational condition as soon as possible by using all available options, including workarounds.

In cases of a Major Incident, its resolution shall be addressed with the highest possible level of urgency, using all resources available at the given time.

3.4.3.5. Request Management

Within the support service hours, the User may submit additional requests to the Provider for the implementation of changes. Changes to the relevant systems are categorized as follows:

- Standard Changes – such changes may be requested by an authorized representative of the User. Requests are submitted through the Span Service Desk using a standardized form.
- Major Changes – such changes are not part of the support service, and following their evaluation, the Provider will prepare a formal offer and delivery timeframes and submit them to the User for review. Upon acceptance of the terms of the Offer, the Provider will proceed with the implementation of the change.

The priority for resolving Standard Change Requests is determined in accordance with the response time table specified for the relevant service.

Requests for Information do not have a defined priority, and the Provider will respond to them on a best-effort basis.

All changes in relation to the current state and configuration of the system are considered project work and must be agreed separately. Furthermore, such work is considered to have a significant impact, and its impact on the existing environment is evaluated.

If changes to the existing IT environment have a significant impact on the services provided, the manner of their performance or their scope, the existing agreement requires revision so that the level of service provided is not jeopardized. Such Major Changes that qualify as project work must be mutually agreed in advance, and a revision of the existing terms and scope of the service provided is mandatory.

Minor Changes and upgrades that do not require more than a few working hours per month per service provided are carried out through the change management process and charged as agreed.

Change Requests received after 15:00 on a business day will be processed on the next business day.

3.4.3.6. Reporting

A regular reporting interval is considered to be one calendar month. During the term of the contracted support, the User will receive a monthly report no later than the 15th day of the current month for the previous month.

The monthly report will in particular include the date of preparation and the period to which it relates, an overview of the total and daily volume of tickets received, classified by type (Incident, Problem, CR, RFI), including average resolution times, as well as a comparative overview of volumes and trends for the preceding period of up to six months.

The report will further include a list of tickets resolved during the reporting period, an overview of problem management activities (proactive and reactive) and, where applicable, improvement proposals and identified risks with a proposal for their mitigation.

In addition, the report will contain an overview of system availability or unavailability, as well as an overview of received requests (change requests and requests for information) together with the corresponding hours spent.

3.4.3.7. Response Times

Prior ity	Name	Description EXAMPLE /	Response	Notification	Escalation
1	Critical	THE BUSINESS SERVICE IS UNAVAILABLE OR COMPROMISED. VIRUSES/MALWARE.	< 60 minutes	Every 60 minutes from the initial response.	After 4 hours from the initial response.
2	High	HIGH IMPACT ON THE BUSINESS SERVICE. Partial unavailability of the business service and/or a large number of users are affected by the incident.	< 120 minutes	Every 120 minutes from the initial response.	After 8 hours from the initial response.
3	Medium	Low impact on the business service. A workaround is available and the impact on end users is minimal.	Within 8 hours	Every 24 hours from the initial response.	After 2 business days from the initial response.
4	Low	Negligible impact on the business service. Comments regarding appearance or form.	Within 24 hours.	Every 48 hours from the initial response.	After 5 business days from the initial response.

All Requests and Incidents are handled during Working Hours. The resolution time or response time for Requests and Incidents received outside Working Hours begins with the next Working Hours period.

Requests for Information are handled on a best-effort basis and the escalation procedure does not apply. Standard Change Requests are treated as tickets with impact level three (3).

With the aim of ensuring a timely response and an appropriate level of attention, Incidents with impact levels 1 and 2 must be reported exclusively by telephone.

3.4.3.8. Prerequisites

For the purpose of fulfilling the obligations set out in this document, the User shall provide the Provider with uninterrupted access to its IT environment and the relevant systems.

In addition to remote access, the Provider also requires administrator privileges on the relevant systems in accordance with the Cybersecurity Requirements.

Within the scope of the agreed service, upon conclusion of the support and maintenance agreement, a current-state assessment will be prepared, covering a review of the Microsoft 365 systems and all related systems that may affect their operation. The current-state assessment will describe the current state of the User's relevant systems, and the estimated time required to prepare the assessment is five (5) working hours. The current-state assessment will not be charged separately, except where the User cancels the service within 12 months from the conclusion of the agreement, in which case the preparation of the current-state assessment will be charged in the amount of EUR 275.00 plus VAT.

3.4.3.9. Limitations

The Authorized Persons referred to in Article 5 of the Master Agreement and other employees authorized by those persons are the only persons authorized to order IT support services.

Support requests received from unauthorized employees of the User will also be recorded; however, their processing will commence only after the User provides the appropriate authorization, whereby response times and any applicable escalation periods begin to run exclusively from the moment such authorization is received.

3.4.3.10. User Satisfaction

User satisfaction represents a key indicator of the quality of the Provider's services, and accordingly, a system has been established for collecting and processing feedback on support and maintenance services.

The User may submit a complaint through the Span Service Desk (+385 1 6690 222), the competent sales representative or the technical support lead, as well as by email at prituzbe@span.eu

The service management system also enables the rating of resolved tickets, whereby participation in the survey is voluntary, and each lowest rating of "1" received for any question is considered a complaint within the meaning of these provisions.

3.4.3.11. The Provider is not responsible for:

- creating backups of user data or storing user documents, archived email messages, etc.;
- costs incurred due to computer hardware failures;
- resolving issues related to unreliability or poor quality of the Internet connection on site. The Provider will detect issues related to the Internet connection and coordinate all activities to resolve such issues on a best-effort basis;

- material or non-material damage caused by force majeure.

All major requests aimed at changes within the IT systems will be agreed outside this Offer and managed as separate projects.

3.4.4. Cybersecurity Requirements

Unless otherwise agreed in writing, the User is solely responsible for taking all necessary steps to protect its IT environment and systems (hereinafter: “Cybersecurity Requirements”), including but not limited to:

- ensuring that all access to the User’s IT environment and systems takes place through Virtual Private Network (“VPN”) solutions or Connection Broker Solutions [direct console access to the User’s internal IT environment is not acceptable];
- ensuring that Multi-Factor Authentication (“MFA”) is required for all external access to the User’s IT environment and systems;
- providing personalized accounts (as opposed to shared accounts) to all Provider employees who require access to the User’s IT environment and systems;
- enabling and enforcing Multi-Factor Authentication (“MFA”) for all accounts connecting to any external interface, including, but not limited to, the account used for access via Virtual Private Network (“VPN”) and accounts used for cloud administration [SaaS, PaaS or IaaS];
- setting the expiration date of passwords for all personalized accounts to no more than one year;
- ensuring that access to the User’s IT environment and systems is granted to all holders of personalized accounts according to the principle of “least privilege”;
- providing separate personalized accounts for on-premise services and cloud services;

The exception to the above rules is the “Break-Glass” account, i.e. an account used in emergencies to access the system or service and which is not available under regular controls. This “Break-Glass” account must be configured for the Provider’s support in accordance with the following requirements: the account must be a permanent member of the required privileged roles [e.g. domain administrators, global administrators];

- the account must not use Multi-Factor Authentication (“MFA”) (i.e. Smartcard or Authentication App);
- the owner of the Break-Glass account must be designated by a specific role within the organization [e.g. the Provider’s support director or the User’s technical lead];
- the password must be long, i.e. at least 16 characters, and must be randomly generated;
- the password must not expire;
- the password must be stored in a physical safe;
- a Chain of Custody must be implemented to ensure secure access;
- the account should be used only for troubleshooting and correcting technical errors that prevent the use of personalized administrator accounts;
- the account password must be changed after each use;

- once every 12 months, the “Break-Glass” account procedure must be tested, meaning that the password must be retrieved, the account must be logged into, the password must be reset and the password must be stored back in the safe.

If the User fails to comply with the Cybersecurity Requirements defined above, the Provider will not be liable for loss of revenue or for any indirect, special, incidental or consequential damage or loss, including loss of use, lost profits, loss of revenue, business interruption or loss of business information, arising from cybersecurity incidents, including, but not limited to:

- unauthorized access to any information system, data or electronic communication network (including a breach of the applicable security policy);
- reduced integrity of an information system, data or electronic communication network;
- unauthorized use of any part of an information system or electronic communication network for the processing (including storage) of data;
- interruption or alteration of the operation (including taking control, malicious disruption and/or denial of service) of an information system or electronic communications network;
- unauthorized changes to embedded programs, software or hardware;
- unauthorized destruction, damage, deletion or alteration of data residing in an information system or electronic communication network;
- removal or restriction of the availability or usability of data residing in an information system or electronic communication network;
- misappropriation, publication, dissemination or any other use of data by persons not authorized to do so.

3.4.5. Difference between SOC Services and Support and Maintenance Services

Support and maintenance services are aimed at ensuring the functionality, maintenance and troubleshooting of the User’s IT infrastructure, software and related systems, within the scope defined by the Offer or the Master Agreement.

Support and maintenance do not include management of the User’s entire IT infrastructure or assumption of responsibility for the overall security of the system, unless this is expressly agreed as a separate service.

The User is solely responsible for establishing, implementing, maintaining and updating its own measures, policies, procedures and technical solutions in the field of information security and cybersecurity.

At the User’s request, the Provider may provide recommendations or proposals related to security measures and good practices; however, such recommendations do not constitute a guarantee or represent an assumption of responsibility for the security of the User’s systems.

The User is aware of and accepts that no information system can be completely secure and that there is always an inherent risk of security incidents, including cyberattacks, unauthorized access and other forms of threat.

Unless expressly agreed otherwise, Support and Maintenance Services do not include cybersecurity services, security monitoring (SOC), security incident management, penetration testing or other specialized security services.

The Provider takes reasonable professional measures when providing the services, including engaging qualified personnel and applying industry good practices, but does not assume responsibility for protecting the User's systems, networks or data against security threats, unauthorized access or other security threats, unless such service has been expressly agreed as a separate service.

4. ORDERING AND CHANGES TO ORDERED QUANTITIES

4.1. Ordering Method and Order Management

IT solutions, products and services are ordered on the basis of an Offer, through an electronic order placed on the Span.Zone platform, by accepting an Offer or by another written or electronic request of the User.

Acceptance of an Offer by the User, as well as a confirmed order, is binding on the parties and forms an integral part of the contractual relationship.

Changes to the quantity or type of subscriptions are possible in accordance with the manufacturer's rules, the type of agreed subscription and these General Terms.

The User is solely responsible for monitoring the duration of its subscriptions for Microsoft and Google products and services and for timely submission of requests for their cancellation.

The Provider may, but is not obliged to, notify the User of the expiry or renewal of a subscription. The absence of such notification does not affect the validity of the subscription renewal and may not constitute grounds for any objection, claim or liability of the Provider, including claims for damages.

For subscriptions that the User independently activates, modifies or cancels through the Span.Zone platform, the User assumes full responsibility for their management, including but not limited to, renewal, modifications and cancellation.

The provisions of this Article take precedence over any other provisions of these General Terms or related documents governing subscription management, except for the Microsoft Customer Agreement, to the extent that they conflict with it.

4.2. Microsoft Products and Services

The quantity and type of Microsoft online services may be ordered or modified upon a written request submitted by an authorized person of the User, specifying the requested services.

The Provider will activate the services or modify the quantity/type of services without undue delay after acceptance of the Offer issued on the basis of the User's request, in accordance with the software manufacturer's rules and these General Terms.

A reduction in the quantity of Microsoft online services applies:

- a) upon monthly subscription renewal – for subscriptions with a monthly term;
- b) upon annual subscription renewal – for subscriptions with an annual term;
- c) upon three-year subscription renewal – for subscriptions with a three-year term;

- d) within 7 (seven) days of activation/increase in quantity – for subscriptions;
- e) within 30 (thirty) days of delivery – for perpetual licenses.

For Microsoft online services, the quantity may only be increased during the subscription term, and the subscription may also be upgraded to a higher-tier license, subject to availability.

Subscriptions for Microsoft software, Azure reservations and Azure Savings are ordered for the entire agreed term and are not subject to changes after activation.

For Azure consumption, the User orders and manages Microsoft Azure resources independently or through requests submitted to the Provider, in accordance with its business needs.

The use of such resources is billed according to the billing model applicable to each individual resource, either based on actual consumption (usage-based model) or according to a pre-agreed commitment model (commitment model), including, but not limited to, models such as Azure Reserved Instances and Azure Savings Plan.

The User may request an increase in the number of resources at any time, and additional resources are included in the billing from the moment of activation. A reduction in resources immediately reduces the charges.

The User is responsible for managing administrator access and controlling the creation of resources within the system. The Provider is not liable for resources activated due to unauthorized or unintended additions by the User or its administrators.

Perpetual software licenses are ordered without a time limit and, after delivery, neither an increase nor a reduction in their quantity is possible.

The User is authorized to independently order and modify the quantities of ordered Microsoft products and services through the Span.Zone platform, in accordance with the software manufacturer's rules. In the event of independent ordering, the User is fully responsible for all consequences of orders placed and/or their cancellation.

4.2.1. Azure Reservations and Azure Savings

The Provider may procure Azure Reservations and Azure Savings services on behalf of the User and in accordance with the User's instructions.

If the User independently activates such services through its own administrator access, the User assumes full financial risk associated with such activation and undertakes to settle all costs incurred in this manner, in accordance with the applicable Microsoft Customer Agreement.

4.2.2. Administrator Privileges

For the provision of Azure services, Azure Reservations, Azure Savings, marketplace services, basic user support and enabling the use of the functionalities of the Span.Zone platform, the User is required to grant the Provider appropriate granular delegated administrator privileges (GDAP), in accordance with Microsoft's recommendation, at a minimum:

- Directory Readers,
- Directory Writers,
- License Administrator,
- Service Support Administrator,

- User Administrator,
- Privileged Role Administrator,
- Privileged Authentication Administrator,
- Helpdesk Administrator,
- Cloud Application Administrator,
- Application Administrator,
- Global Reader.

GDAP privileges are granted for a period of up to 730 (seven hundred and thirty) days and are automatically extended for an additional 6 (six) months, unless previously revoked by the User.

The User is entitled to revoke the administrator privileges granted to the Provider at any time.

In the event of revocation of administrator privileges, including, but not limited to, the revocation of GDAP privileges, the functionalities of the Span.Zone platform and related services will be limited exclusively to basic purchasing functions, while further administration, resource management, technical support and other advanced functionalities will not be available.

If the User revokes or does not grant the Provider GDAP privileges, the User acknowledges and agrees that the Provider will no longer have authorized access to the User's Tenant or the ability to submit requests to or communicate with Microsoft on behalf of the User. Consequently, in the event of loss of access credentials for the Tenant, such situation cannot be resolved by the Provider within the scope of the regular service. Any potential resolution of the aforementioned situation may be initiated exclusively as a separate service, subject to a separate fee, which will be defined in the relevant Offer.

The User is specifically informed and agrees that, in such case, the Span.Zone platform functions exclusively as a sales interface (web shop) for the purchase of licenses and/or services, without the possibility of further management of such licenses and/or services through the Provider.

The Provider assumes no responsibility for limitations in the use of services, inability to administer, interruptions in operation, loss of functionality, loss of data, loss of profit or any other direct or indirect damage that may arise as a consequence of the revocation of administrator privileges.

The User expressly accepts all consequences arising from such revocation, including the need for independent management of resources and any additional costs or risks associated therewith.

4.3. Google Products and Services

4.3.1. Google Workspace

The User may request an increase in the number of licenses at any time. Additional licenses are activated upon receipt of the request and are included in the billing from the moment of activation.

The User also agrees that adding new user accounts or assigning licenses within the Google Workspace administrator interface may result in an automatic increase in the number of active licenses. All licenses activated in this manner are deemed duly ordered and are subject to billing, regardless of whether a request for an increase was previously submitted to the Provider.

A reduction in the number of licenses is possible exclusively in accordance with the selected subscription model:

- In the case of a flexible (monthly) model, the reduction is possible and applies from the following billing period;
- In the case of an annual model with a commitment term, a reduction in the number of licenses is not possible during the agreed period, but only upon its expiry.

The User is responsible for managing administrator access and controlling the assignment of licenses within the system. The Provider is not liable for any licenses activated due to unauthorized or unintentional addition of users by the User or its administrators.

The Provider reserves the right to perform a calculation at the end of the billing period to ensure that all active licenses are properly calculated and invoiced.

For the purpose of protecting the Provider's interests, the number of licenses may be capped as agreed in the commercial Offer. The User is required to request all changes to the number of licenses in a timely manner through the designated communication channel with the Provider.

4.3.2. Google Cloud Platform

The User orders Google Cloud Platform (GCP) resources in accordance with its business needs, whereby each resource is charged based on actual consumption (usage-based).

The User may request an increase in resources at any time, and additional resources are included in the billing from the moment of activation.

The User agrees that creating new resources within the administrator interface may result in an automatic increase in charges. All billing units activated in this manner are deemed duly ordered and are subject to billing, regardless of whether the request was previously submitted to the Provider.

A reduction in resources is automatically reflected in the charges.

The User is responsible for managing administrator access and controlling the creation of resources within the system. The Provider is not liable for any resources activated due to unauthorized or unintended additions by the User or its administrators.

4.3.3. GCP Commitment Models

The User may use Google Cloud Platform (GCP) resources through Committed Use Discounts (CUD), whereby the User undertakes to use a predetermined number of resources for the duration of the commitment, without the possibility of reducing the resources during that period.

Sustained Use Discounts (SUD) are applied automatically to resources that are used continuously, without a commitment requirement, with the possibility of freely increasing or reducing the resources.

The User is responsible for managing administrator access and controlling the creation of resources within the system, and accepts that CUD resources cannot be reduced while the agreed period is in effect, whereas SUD resources may be freely increased and reduced.

4.3.4. Google Cloud Identity

The User may order Google Cloud Identity licenses according to its needs, whereby licenses are assigned per user account. Adding new user accounts or assigning licenses within the administrator interface may automatically increase the number of active licenses, which are charged immediately.

A reduction in the number of licenses is possible in accordance with the subscription model and applies from the following billing period. The User is responsible for managing administrator access, and the Provider is not liable for any unintentional or unauthorized addition of licenses.

4.3.5. Google Chrome

The User orders Google Chrome Enterprise licenses according to its business needs, whereby licenses are assigned per user account or device, depending on the subscription model.

The User may request an increase in the number of licenses at any time, and such licenses are immediately included in the billing from the moment of activation.

Adding new user accounts or devices within the administrator interface may result in an automatic increase in the number of active licenses. All licenses activated in this manner are deemed duly ordered and are subject to billing, regardless of whether the request was previously submitted to the Provider.

A reduction in the number of licenses is possible in accordance with the selected subscription model and applies from the following billing period.

The User is responsible for managing administrator access and controlling the assignment of licenses within the system, and the Provider is not liable for licenses activated due to unintentional or unauthorized addition by the User.

4.4. Support and Maintenance

The User shall use the support and maintenance services in accordance with the scope, parameters and terms defined in the accepted Offer.

Requests for the provision of support and maintenance are submitted in the manner and through the communication channels defined in the Offer or in these General Terms.

5. PRICES AND BILLING

5.1. Pricing Method

The prices of IT Solutions and Services are determined in accordance with the accepted Offer, the Provider's and/or manufacturer's applicable price list at the time of ordering, service activation or usage billing, depending on the type of product or service.

Unless otherwise stated, prices are expressed exclusive of value-added tax (VAT). VAT is calculated and charged in accordance with applicable regulations.

5.2. Microsoft Products and Services

5.2.1. Price Definition and Quantity Billing

The prices and quantities of initially ordered Microsoft products and services are defined in the accepted Offer. All subsequent orders and changes are determined in separate Offers.

The Provider guarantees that the price of Microsoft online services remains unchanged from the time of activation until the cancellation or renewal of the service term, whichever occurs earlier.

The prices of Microsoft online services with monthly, annual or three-year subscriptions are adjusted upon subscription renewal according to the applicable Microsoft price list in effect at the time of renewal.

Billing for Microsoft online services may include:

- billing for services for the current period based on the status as of the first day of the billing period;
- billing for other agreed services for the current period at the User's request;
- billing for differences in the quantity of services for the previous period that were not billed on the previous invoice.

The prices of subscriptions to Microsoft software, Azure Reservations, Azure Savings and perpetual software licenses apply according to the applicable Microsoft price list in effect at the time of ordering.

5.2.2. Azure Consumption

Azure service prices are billed based on actual consumption, in accordance with the official Microsoft Azure report and the applicable Microsoft price list in effect at the time of billing.

If the User modifies, limits or revokes the administrator privileges granted to the Provider, this may affect the possibility of obtaining contractual benefits and discounts from the manufacturer or supplier; therefore, the Provider reserves the right to appropriately adjust the applicable commercial terms.

Upon the occurrence of the circumstances referred to in the preceding paragraph, the User accepts that, as a result thereof, the previously approved commercial terms cease to apply. In such case, the Provider has the right to subsequently bill the price difference for services already provided or products already delivered, applying the applicable full prices without approved discounts, and to charge such difference to the User. The Provider will notify the User of the above circumstances and the resulting price adjustment within a reasonable period from the time the Provider becomes aware of them.

5.3. Google Products and Services

5.3.1. Google Workspace Subscriptions

The prices of Google Workspace licenses are determined according to the selected plan and the number of users.

5.3.2. Google Cloud Platform

The prices of Google Cloud Platform services are billed according to actual consumption, in accordance with the official price list in effect at the time of billing.

The prices of GCP commitment models are determined according to the agreed number of resources and the type of discount:

- Committed Use Discounts (CUD) – the fee is based on the predetermined number of resources agreed for the duration of the commitment, without the possibility of reducing the resources during that period;
- Sustained Use Discounts (SUD) – the discount is automatically applied to resources that are used continuously, and the price is billed in real time, with the possibility of freely increasing or reducing the resources.

The prices of Google Cloud Identity licenses are determined according to the selected plan and the number of users.

The prices of Google Chrome Enterprise licenses are determined according to the selected plan and the number of users or devices.

5.4. Support and Maintenance

The price of IT support services is billed according to the actual working hours spent, in accordance with the prices defined in the accepted Offer.

The minimum billing unit for interventions via remote access is 0.5 (half) an hour, while the minimum billing unit for working hours for interventions resolved at the User's location is two (2) hours.

After the minimum billing unit, billing is performed for each commenced 15 (fifteen) minutes, in accordance with the applicable price list for professional staff defined in the Offer.

5.4.1. Professional Staff Price List

Hours spent resolving requests are billed according to the applicable professional staff price list, in accordance with the Offer submitted at the User's request.

The stated prices apply to interventions during Working Hours. For interventions outside Working Hours, the price is increased by 50%, while for night work and work on weekends, the price is increased by 100%.

For interventions at locations outside Zagreb, the Provider is entitled to separately charge the actual costs of transportation, tolls, daily allowances and overnight stays.

6. PAYMENT

6.1. Payment Terms and Method

6.1.1. Payment Deadlines and Method

The User undertakes to pay the issued invoices within 30 (thirty) days from the date of invoice issuance, unless otherwise stated in the Offer or on the invoice.

Unless otherwise specifically stated in the Offer or another document, the User will make payments for the IT support services provided to the Provider's account no. HR4324070001100472815 held with OTP banka d.d.

6.1.2. Currency, Exchange Rate and Conversion

All prices and fees under the Master Agreement are generally expressed and charged in euros (EUR), unless expressly otherwise stated for a particular service or market in the Offer, purchase order or other contractual document.

In cases where the Provider's input costs are tied to another currency (e.g. USD), or where the contractual relationship applies outside the European Economic Area (EEA), the Provider reserves the right to express prices and/or charge in another currency. In such cases, the applicable exchange rate, conversion method and reference source of the exchange rate will be specified in the Offer or another relevant document provided to the User.

Unless otherwise agreed, currency conversion will be performed using the selling exchange rate of the Provider's business bank applicable on the date of invoice issuance, or another reasonably selected reference exchange rate applied by the Provider in its regular business operations.

The User agrees to bear the risk of exchange-rate changes between the currency in which the prices were initially expressed and the payment currency, unless expressly agreed otherwise. The Provider is not liable for any differences arising from exchange-rate changes or payment transaction costs.

This provision applies to all territories, whereby the local currency or another currency determined by the Provider will apply to markets outside the EEA, in accordance with applicable regulations and business practice.

6.2. Microsoft Products and Services

Payment for Microsoft online services and subscriptions to Microsoft software is made:

- as a one-time payment for the entire subscription period, or
- periodically (monthly, annually),

in accordance with the accepted Offer and the type of subscription.

The invoice for the services provided and/or products delivered is issued exclusively to the User, as the Contracting Party that entered into the Master Agreement, accepted these General Terms and entered into the relevant manufacturer's customer agreement, and that is also the owner of the respective Tenant.

The User's affiliates, within the meaning of the provisions of the Companies Act, may use the services and/or products exclusively through the User as the holder of the contractual relationship, whereby all invoices are issued exclusively to the User and not to affiliates or third parties. The User is authorized to allocate costs internally among the affiliates within its group.

The User is not authorized to resell and/or commercially distribute the services to third parties, including its own affiliates, unless this is permitted by the manufacturer's rules or specifically agreed otherwise.

The invoice is delivered to the User no later than the 15th day of the month.

The invoice contains an overview of the products delivered and services provided by individual items. More detailed information in the form of structured reports (e.g. by affiliates, organizational units or other cost centers) may be available to the User through the Span.Zone platform as an additional service.

The aforementioned additional service is charged at a separate fee determined upon the User's request, in accordance with the Provider's applicable price list. For the purpose of using the relevant service, the User is required to ensure appropriate access to the platform within its Tenant, as a technical prerequisite for the provision of the service.

Payment for Azure Reservations and Azure Savings is made monthly based on an invoice issued by the Provider and delivered to the User no later than the 15th (fifteenth) day of the month during the period of use, or as a one-time payment for the entire period of use.

Payment for perpetual software licenses is made as a one-time payment, based on an issued invoice delivered to the User no later than 15 (fifteen) days after delivery of the product.

In the event of suspension of access to the service, the User undertakes to continue making ongoing payments for the subscription service in accordance with the provisions of these General Terms.

The provisions of these General Terms relating to the User's obligations concerning payment for the subscription service continue to apply in the event of termination of this contractual relationship in any manner for the entire agreed subscription period and until its expiry.

6.3. Google Products and Services

Payment for Google products and services is made monthly or annually, depending on the subscription model, based on an invoice issued at the end of the month for the products and services used during the preceding billing period.

In the event of suspension of access to the services, the User is required to continue making all ongoing payments for the subscription services in accordance with the provisions of these General Terms.

The provisions of these General Terms relating to the User's obligations concerning payment for the subscription service continue to apply in the event of termination of the contractual relationship in any manner for the entire agreed subscription period and until its expiry.

6.4. Support and Maintenance

Support and maintenance services are paid for monthly, according to the services actually performed and hours spent during the preceding month, based on invoices issued by the Provider.

6.5. Consequences of Non-Payment

In the event of late payment, the Provider has the right to:

- charge statutory default interest;
- temporarily limit or suspend access to the services;
- suspend the delivery of products and services and refuse further deliveries;
- terminate the contractual relationship while retaining the right to collect all due and future obligations for the agreed subscription period.

Suspension of the IT Solutions and Services due to non-payment does not release the User from the obligation to pay for the agreed subscription period.

Payment obligations for the agreed subscription period remain in force even in the event of termination of the contractual relationship in any manner, until the expiry of the agreed subscription period.

7. CUSTOMER SUPPORT AND COMMUNICATION

7.1. Scope of Customer Support

The Provider will provide the User with customer support in connection with the use of the Span.Zone platform and Microsoft and Google products and services, including receiving and processing User requests related to the quantity and type of the aforementioned products and services, to the extent that the Provider reasonably considers customary for customer inquiries.

For requests that exceed the aforementioned scope of support, the Provider has the right to charge for customer support services in accordance with the applicable price list.

7.2. Contact Persons

The User is authorized to update and change the details of the Authorized Persons specified in the Master Agreement.

For updating the details and/or changing the Authorized Persons for the performance of the agreement, a notice delivered to the Provider will be sufficient if submitted:

- (i) from the email address of the existing Authorized Person;
- (ii) by a person authorized to represent the User within the meaning of applicable regulations.

The Provider has the right to rely on the notice received without any further verification of authority and is not liable for the consequences of acting in good faith based on such notice.

7.3. Microsoft Products and Services

The Provider will provide customer support for the following products and services:

- subscriptions to Microsoft online services;
- Microsoft software subscriptions;
- Azure:
 - Azure consumption;
 - Azure Reservations;
 - Azure Savings;
 - Azure Marketplace.
- Microsoft perpetual licenses.

For the Microsoft products and services referred to in the preceding paragraph of this Article that are purchased from the Provider, customer support within the scope of free support, subject to the assignment of the recommended GDAP roles referred to in Article 4.2.2, includes:

- a. creation of the organization (setting up the Client's account);

- b. delivery of licenses;
- c. creation of an administrator account and delivery of access credentials;
- d. verification of the operational status of Microsoft online services.

If the User does not assign the required GDAP roles, the limitations referred to in Article 4.2.2 of these General Terms will apply.

The Provider reserves the right to charge a fee for support that is not covered by the scope of free support, in accordance with the applicable price list.

Upon termination of the Master Agreement, the User loses the right to free support related to Perpetual Software Licenses, while the Provider may continue to provide support for a fee in accordance with the applicable price list.

7.4. Method and Timing of Support Provision

Technical Support is available during working hours.

A support request may be submitted exclusively by a person authorized to represent the User, an Authorized Technical Person, or another person authorized by either of them.

8. CONFIDENTIALITY AND NON-DISCLOSURE

The terms of the Master Agreement, as well as all other information that other persons become aware of during the performance of the Master Agreement, constitute confidential information and must be kept confidential with due professional care. Without the specific written approval of the other Contracting Party, neither Contracting Party is authorized to provide and/or disclose any information relating to this agreement to any third party.

The parties to this contractual relationship confirm that:

- any disclosure of confidential information to a third party without the prior express approval of the other Contracting Party is excluded, except to the extent necessary to fulfill legal obligations or for the purposes of an audit and/or tax inspection;
- they will not disclose any information about the other Contracting Party that is not generally known to the public and that is in any way related to the business of the other Contracting Party;
- they will not copy or reproduce, in any form, any information they become aware of during the performance of their obligations under this contractual relationship if such reproduction does not serve the purpose provided for under this contractual relationship.

In the event of unauthorized disclosure of confidential information, the Contracting Party responsible for such disclosure is required to compensate the other Contracting Party for all actual damages arising from such conduct.

The parties to this contractual relationship undertake to ensure that all third parties, such as employees, associates, users, and other persons connected with either of the Contracting Parties, who, based on a valid legal basis, have access to the provisions of this agreement, are informed of the confidentiality provisions set out in this Article and that such third parties maintain confidentiality in the same manner as the Contracting Parties.

These confidentiality provisions remain in effect for 5 (five) years after termination of this contractual relationship.

Notwithstanding the preceding provisions of this Article, the User consents to the Provider using basic information about the contractual relationship for the purpose of demonstrating the Provider's business experience and references, including in public and private procurement procedures and in other business and promotional materials.

For this purpose, the Provider is authorized to use only the following information:

- the User's name (company name) and address;
- a general description of the IT products and services provided;
- the type and scope of the services provided;
- the total agreed value (or value range);
- the duration of the contractual relationship.

The Provider undertakes to use the aforementioned information exclusively for the purpose of demonstrating business experience and references, in a manner that does not disclose the User's trade secrets or other confidential information not covered by this Article, with due professional care and in accordance with applicable regulations.

9. FORCE MAJEURE

Neither party to this contractual relationship is liable for non-performance or delayed performance of its contractual obligations if such non-performance or delay is the result of circumstances of force majeure.

For the purposes of these General Terms, force majeure means extraordinary, unforeseeable, and unavoidable circumstances that arise after the conclusion of this contractual relationship and that the Contracting Party could not prevent, remedy, or avoid by taking reasonable measures, including, but not limited to: natural disasters, war, terrorist acts, riots, large-scale strikes, epidemics and pandemics, decisions or measures of competent authorities, disruptions in the supply of energy or communications networks, as well as serious disruptions in the operation of third-party IT or telecommunications infrastructure.

The party to this contractual relationship affected by force majeure is required to notify the other Contracting Party, without delay and no later than within a reasonable period, of the occurrence of the force majeure circumstances, their nature, expected duration, and impact on the performance of contractual obligations.

During the period of force majeure, the obligations of the Contracting Party affected by force majeure are suspended to the extent that they cannot be performed due to the occurrence of such circumstances, without the other party being entitled to damages or a contractual penalty.

The Contracting Party affected by force majeure is required to take all reasonable measures to mitigate the consequences of force majeure and resume performance of its contractual obligations as soon as the circumstances permit.

If the force majeure circumstances continue uninterrupted for more than ninety (90) days, either Contracting Party has the right to terminate the Master Agreement by written notice to the other party, without any obligation to pay damages, whereby such termination does not affect obligations that became due by the date of termination.

The occurrence of force majeure does not release the User from the obligation to pay due and undisputed monetary obligations incurred before the occurrence of the force majeure circumstances, unless expressly agreed otherwise or required by mandatory regulations.

The provisions of this Article apply and are interpreted in accordance with the principle of good faith and fair dealing.

10. PERSONAL DATA PROCESSING

The Provider undertakes not to access or otherwise process the controller's personal data at any time, except on the basis of the User's prior written instruction as the controller of personal data, within the meaning of the provisions of the General Data Protection Regulation.

The Provider undertakes to process the data exclusively in the manner and to the extent necessary for the performance of its obligations under the Master Agreement.

The Contracting Parties mutually acknowledge that they have defined the details of the processing of personal data in the Personal Data Processing Agreement (Annex 1), which forms an integral part of these General Terms.

11. COMMENCEMENT AND DURATION OF IT SOLUTIONS AND SERVICES

11.1. General Commencement of the Contract Term and Automatic Renewal

The provision of IT Solutions and Services commences on the date of delivery of the first solution and/or service, unless otherwise expressly provided for an individual IT Solution or Service in this Article.

The agreement is concluded for the duration of the services as defined in Article 3 of these General Terms.

Where the subject matter of the agreement is a subscription to IT Solutions and/or Services, including support and maintenance services, the agreement automatically renews for successive subscription periods of the same duration, unless either Contracting Party terminates the agreement in writing no later than 30 (thirty) days before the expiration of the current subscription period.

11.2. Microsoft Products and Services

The provision of Microsoft services commences on the date of delivery of the service and products through the Microsoft administrative portal and continues for the duration of the subscription period, while perpetual licenses are granted without a time limit, in accordance with the manufacturer's terms.

In the case of a combination of Perpetual Software Licenses and a subscription to Microsoft services, the subscription period for Microsoft services is treated separately from the term of the agreement relating to Perpetual Software Licenses, and the User is authorized to change subscription quantities in accordance with these General Terms.

Upon purchase of Perpetual Software Licenses, the Microsoft Customer Agreement remains in effect for the entire duration of the licenses, and any termination of the Master Agreement does not affect the validity of the Microsoft Customer Agreement.

11.3. Google Products and Services

The provision of Google products and services commences on the date specified in the applicable Offer and continues for the period specified in that Offer or, as applicable, in these General Terms.

11.4. Support and Maintenance

Support and maintenance services commence on the date specified in the applicable Offer and are provided for a period of 12 (twelve) months, unless otherwise specified in the Offer.

12. INTELLECTUAL PROPERTY RIGHTS

12.1. Ownership of IT Solutions and Services

All copyrights, related rights, industrial property rights, trade secret rights, know-how, and other intellectual property rights relating to the IT Solutions and Services that are the subject of these General Terms belong exclusively to their respective manufacturers or rights holders (e.g., Microsoft, Google, and others), unless expressly stated otherwise.

The Provider does not acquire or transfer ownership of such rights, but enables the User to acquire rights to use them in accordance with the manufacturer's license terms and the accepted Offer.

In the case of services independently developed by the Provider (e.g., documentation, reports, configurations, scripts, or other deliverables), the intellectual property rights in such materials belong to the Provider, unless otherwise agreed.

12.2. Scope of the Right of Use

These General Terms do not transfer ownership of the IT Solutions and Services to the User, but exclusively the right of use:

- for perpetual licenses – a non-exclusive, non-transferable, and unlimited right of use;
- for subscription licenses – a non-exclusive, non-transferable, and time-limited right of use;

all within the scope and duration, and subject to the terms, set out in the manufacturer's licensing terms, the Master Agreement, and these General Terms.

The User is required to comply with all applicable manufacturer licensing terms, including the Microsoft Customer Agreement or other relevant manufacturer agreements.

12.3. Restrictions on Use

The User undertakes that, without the prior express written consent of the rights holder, except to the extent permitted by mandatory regulations, it will not:

- a) reproduce, modify, adapt, translate, decompile, disassemble, or otherwise attempt to discover the source code of the IT Solutions or Service deliverables;
- b) remove, modify, or conceal copyright notices, trademarks, or other intellectual property rights notices;
- c) sublicense, lease, rent, or otherwise make products or licenses available to third parties, unless expressly permitted by the manufacturer's licensing terms;

- d) use the IT Solutions and Services in a manner that could result in an infringement of the intellectual property rights of the manufacturer, the Provider, or third parties.

12.4. Responsibility for User Content

The User is solely responsible for the legality, accuracy, and content of all data, information, and materials that it enters, processes, stores, or otherwise uses through the IT Solutions and Services.

The User warrants that such use does not infringe the rights of third parties, including intellectual property rights, and undertakes to compensate the Provider for any damage or cost incurred as a result of the infringement of such rights.

12.5. Infringement of Intellectual Property Rights

In the event of suspected infringement of intellectual property rights, the Provider has the right to take the necessary measures to prevent further infringement, including temporarily suspending access to the services.

If a third party asserts a claim based on an alleged infringement of intellectual property rights related to the manufacturer's digital products, liability for such infringement is governed by the manufacturer's terms.

12.6. Duration of Provisions

The provisions of this Article remain in effect and continue to have legal effect even after the termination of the contractual relationship, regardless of the legal basis for such termination.

13. WARRANTY AND LIABILITY

13.1. Exclusion of Warranties

IT Products and Services are made available to the User on an "as-is" and "as-available" basis, unless expressly agreed otherwise in writing. The Provider gives no additional warranties, whether express or implied, including warranties of uninterrupted operation, availability, error-free performance, or fitness for the User's particular purpose, except as expressly stated in these General Terms.

13.2. Third-Party Products and Services

The Provider assumes no liability for third-party products and services ordered by the User under the Master Agreement, to the fullest extent permitted by law. Third-party products and services are governed by separate terms of use (T&Cs, EULAs, etc.) and are subject to the User's relationship with the respective manufacturer or supplier.

13.3. Limitations on the Provision of Services and Exclusion of Liability

The Provider is not obligated to remedy defects resulting from:

- changes, modifications, or interventions in software or customizations performed by the User;
- the installation, integration, or use of third-party software, add-ons, or components;
- requirements or functionalities outside the scope defined by these General Terms.

The Provider is not liable for:

- damage resulting from incorrect or unlawful use of IT Products and Services;
- damage caused by inaccurate, incomplete, or delayed data;
- damage resulting from errors in third-party software;
- interruptions, restrictions, or unavailability of IT Products and Services or third-party systems;
- loss of profits, loss of data, loss of business opportunities, or any consequential or indirect damages.

13.4. Limitation of Liability

The Provider's liability for damage, regardless of the legal basis, is limited to damage caused intentionally or by gross negligence.

The Provider's total monetary liability for all claims related to IT Products and Services is limited to the amount of fees actually paid by the User to the Provider during the twelve (12) months preceding the occurrence of the damage.

The limitations and exclusions of liability set out in this Article do not apply if they would be contrary to mandatory regulations of the Republic of Croatia.

13.5. Indemnification and Duration of Provisions

The User undertakes to indemnify and hold the Provider harmless from all third-party claims, damages, costs, and liabilities arising from:

- unlawful or unauthorized use of IT Products and Services;
- breach of these General Terms by the User;
- infringement of third-party rights in connection with data or content processed by the User through the use of IT Products and Services.

The provisions of this Article remain in force even after the termination of the contractual relationship, regardless of the reason for such termination.

13.6. Suspension, Restriction or Denial of Services

The Provider has the right, at any time and without prior notice, in the cases provided for under these General Terms (including, but not limited to, non-payment, breach of contractual obligations, security reasons, or non-compliance with the terms of use), to temporarily or permanently suspend, restrict, or deny access to IT Products and Services in full, without any obligation to provide compensation or assume liability toward the User.

To the fullest extent permitted by law, the Provider has no liability for any damage, loss, or cost that may be incurred by the User or third parties as a result of such suspension, restriction, or denial of access, including, without limitation, loss of or damage to data, loss of profits, revenue, or business opportunities, business interruption, disruption of contractual relationships, or any direct, indirect, incidental, or consequential damages, regardless of whether the Provider was advised of the possibility of such damage.

The User expressly acknowledges that it is solely responsible for ensuring the continuity of its business, including regularly making backups and implementing appropriate technical and organizational measures to mitigate risks, and waives any claims against the Provider arising from any suspension or restriction of services carried out in accordance with this Article.

The provisions of this Article apply regardless of the legal basis of the claim and remain in force even after the termination of the contractual relationship.

14. TERMINATION AND CESSATION OF USE

Each Contracting Party has the right to terminate the Master Agreement in writing, without stating any reason, subject to a notice period of 30 (thirty) days.

The User has the right to terminate the use of an individual service covered by the Master Agreement, without affecting the continued validity of the contractual relationship in relation to the other agreed services. All provisions of this Article relating to termination of the contractual relationship apply accordingly to such termination, unless the nature of an individual provision indicates otherwise. In such case, references to the agreement or contractual relationship are interpreted as references to the part of the agreement or contractual relationship relating to that service.

Each Contracting Party has the right to terminate the Master Agreement in writing without a notice period in the following cases:

- a breach of the contractual provisions committed by the other Contracting Party, provided that it has notified the other party in writing of the identified breach and that the other party has failed to remedy the identified breach within 14 (fourteen) days of receipt of the notice;
- if bankruptcy or liquidation proceedings are opened against the other Contracting Party, or if it becomes insolvent, in which case the right to terminate applies to the contractual relationship in its entirety.

If, within the above period, the breaching party fails to bring its conduct into compliance with its contractual obligations, the contractual relationship, or the part of the contractual relationship relating to an individual service, is deemed terminated upon expiry of the additional period, without the need for any further notices or declarations.

In the event of termination of a part of the Master Agreement or of the Master Agreement in its entirety, the Contracting Parties undertake to settle their mutual claims relating to obligations already performed within the scope of this contractual relationship, no later than within 30 (thirty) days from the date of termination.

The Contracting Parties agree that notices of default and/or termination are sent by registered mail with return receipt to the addresses specified in the header of the Master Agreement or by e-mail to the Authorized Contact Persons. Delivery is deemed to have been made on the date on which the registered mail is handed over to the postal service or on the date on which the e-mail is received, or on the first following working day if the e-mail is received on a non-working day.

In the event of a change of business address, each Contracting Party is obliged to notify the other Contracting Party of such change no later than fifteen (15) days after the date of the change of business address.

15. ANTI-CORRUPTION CLAUSE

The User undertakes to fully comply with all applicable regulations on the prevention of corruption and money laundering in implementing the provisions of the Master Agreement and not to take, directly or indirectly, any action that could cause a breach of any applicable anti-corruption regulation or regulation on the prevention of money laundering, including the Provider's rules governing the aforementioned areas and published on the Provider's website.

The User has read and agrees to the provisions of the Provider's Code of Business Conduct available at: <https://www.span.eu/hr/o-nama/kodeks-poslovnog-ponasanja/>.

This obligation applies in particular to unlawful payments or the provision of gifts for the purpose of obtaining an undue benefit for any representative, intermediary or third party acting in the name and on behalf of either Contracting Party, and in particular to public officials, members of their families or their close associates.

The Contracting Parties will notify each other without delay if they become aware of or have a specific suspicion of any act of corruption in relation to the negotiation, conclusion or performance of this contractual relationship or other legal transactions arising from this contractual relationship.

In the event of a breach or non-compliance with the provisions of this Article or any applicable regulation on the prevention of corruption and money laundering, the Contracting Party acting in accordance with the agreement has the right to terminate this contractual relationship at any time, while making a claim for compensation in the full amount of the damage incurred against the party that committed the corrupt acts.

16. USER REPRESENTATIONS AND COMPLIANCE (KYC AND SANCTIONS)

By accepting these General Terms, the User represents and warrants that:

- a) neither the User nor any person that directly or indirectly controls the User (including its beneficial owners, members of its management board or related persons) is subject to international sanctions (including, but not limited to, sanctions imposed by the European Union, the United Nations, OFAC and the United Kingdom), nor is the User or any such person included on any applicable sanctions list;
- b) the User is not directly or indirectly owned or controlled by any sanctioned person;
- c) the User is not a politically exposed person (PEP) and is not controlled by such a person or, if this status applies, it has been fully disclosed to the Provider in advance;
- d) the funds used by the User to pay for IT products and services do not originate from unlawful activities, including money laundering, corruption or terrorist financing;
- e) the User shall not use IT products and services in a manner that would directly or indirectly enable access to, use of, or disposal of IT products and services by persons or entities subject to sanctions or located in sanctioned jurisdictions;
- f) the User shall not assign, transfer or enable third parties to use IT products and services contrary to applicable regulations, including regulations on international sanctions;
- g) the User is not aware of any circumstances that could affect its compliance status with respect to regulations on the prevention of money laundering, international sanctions or financial crime that have not been disclosed to the Provider;
- h) at the Provider's request, the User shall provide information regarding the end users, the location of use and beneficial owners;
- i) all data and information provided to the Provider are accurate, complete and up to date, and the User undertakes to notify the Provider without delay, and no later than within 2 (two) working days, of any change that may affect these representations.

The User agrees that, during the term of the Master Agreement or, in the case of perpetual licenses, the Provider may conduct checks of the User, its beneficial owners and related persons against sanctions lists, PEP registers and other relevant sources on an ongoing basis.

The User is required to use IT products and services in accordance with all applicable laws and regulations, as well as the manufacturer's rules and requirements, particularly those relating to sanctions, export restrictions and acceptable use of services.

In the event of a breach of this provision, or if the Provider determines or reasonably suspects such a breach, or if required by applicable regulations or the manufacturer, the Provider has the right, without liability to the User, to:

- immediately suspend the provision of IT products and services, in whole or in part; and/or
- terminate the Master Agreement with immediate effect.

A breach of this provision is considered a material breach of the Master Agreement.

The Provider has the right to refuse to accept an order, postpone or refuse delivery if screening or a request from the manufacturer, distributor, bank or competent authority indicates a risk relating to sanctions, AML, export control or reputation.

17. GOVERNING LAW AND JURISDICTION

The Contracting Parties undertake to primarily attempt to resolve all disputes, disagreements or claims arising from or in connection with these General Terms or the Master Agreement amicably, in good faith and through direct negotiations.

For the purpose of amicable dispute resolution, the party that considers that a breach of contractual obligations has occurred is required to send the other party a written notice describing the dispute and proposing a method for its resolution, and to allow a reasonable period, which may not be shorter than thirty (30) days, for a response and an attempt to resolve the dispute amicably.

If the Contracting Parties fail to resolve the dispute amicably within the period referred to in the preceding paragraph, either of them has the right to initiate appropriate court or other proceedings for the protection of its rights.

These General Terms and the Master Agreement are governed by and construed in accordance with the laws of the Republic of Croatia.

For the resolution of all disputes arising from or in connection with the Master Agreement, the exclusive subject-matter and territorial jurisdiction of the competent court in Zagreb is agreed.

The obligation to attempt to resolve a dispute amicably does not exclude the right of either Contracting Party, where necessary, to seek interim or protective measures before the competent court without delay.

18. AMENDMENTS TO THE GENERAL TERMS

The Provider reserves the right to unilaterally amend or supplement these General Terms, in particular in the event of amendments by the software manufacturer, changes to applicable regulations, changes in business operations and similar circumstances.

The Provider shall notify the User of any amendments or supplements to the General Terms by publishing the amended General Terms on its website. The Provider may, but is not required to, at its own discretion, additionally notify the User of such amendments by e-mail or by other means.

Amendments to the General Terms are published at least 30 (thirty) days before they enter into force, unless such amendments are necessary for compliance with mandatory regulations, in which case they may enter into force earlier.

The User is deemed to have been duly notified of amendments and supplements to the General Terms at the time they are published on the Provider's website.

The User is deemed to have accepted the amended General Terms if, after the date on which they enter into force, the User continues to use the IT Solutions and/or Services or fails to submit a written objection to the Provider within 14 (fourteen) days from the date on which they enter into force.

If the User does not accept the amended General Terms, the User has the right, no later than 7 (seven) days before the amendments enter into force, to terminate the Master Agreement with effect as of the date on which the amendments enter into force, provided that such termination does not affect obligations that have become due and payable up to the date of termination of the Master Agreement, or obligations that become due in accordance with the applicable licensing terms.

19. FINAL PROVISIONS

If any provision of these General Terms proves to be null and void, invalid or unenforceable, in whole or in part, such nullity, invalidity or unenforceability shall not affect the validity and enforceability of the remaining provisions of these General Terms.

The Provider undertakes to replace the null and void, invalid or unenforceable provision without delay with a valid and enforceable provision that most closely corresponds, in its legal and economic purpose, to the original intention of such provision.

Until the replacement pursuant to the preceding paragraph, these General Terms are to be interpreted and applied to the greatest possible extent in a manner that enables their continued valid and lawful application.

These General Terms enter into force on 1st of October 2026.

Annex I

DATA PROCESSING AGREEMENT

(Agreement)

This Agreement is entered into between:

the User (“Controller”),

and

the Provider (“Processor”),

(the Controller and the Processor hereinafter individually: **“Party”**, and jointly: **“Parties”**).

Definitions

In this Agreement, the following words and expressions shall have the following meanings:

Controller	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 and is identified on the first page on this agreement.
Instruction	written instruction, issued by the Controller to the Processor, regarded to Personal Data, or any other written instructions of the Controller to the Processor.
Master Agreement	has the meaning assigned to it in clause 1.1 of this Agreement.
National Law	any applicable national data protection law from a member state of the European Union.
Personal Data	any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; where provided for by National Law, also data relating to legal persons and entities qualifies as Personal Data, to the extent mandatory.
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;
Processing or Process	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;
Processor	natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller and is identified on the first page on this agreement.
Regulation	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;

1. OBJECT OF THIS AGREEMENT

1. The Parties concluded the Agreement on the delivery of IT solutions and provision of IT services on [please insert the date on which the master agreement was concluded] ("*Master Agreement*"). For the purpose of performing the Parties' obligations arising from the Master Agreement, the Processor will have to Process certain Personal Data on behalf of the Controller ("*Controller Data*").
2. This Agreement specifies the data protection related rights and obligations of the Parties in relation to Processing of Controller Data by the Processor for the purpose of performing their rights and obligations arising from the Master Agreement.

2. SCOPE OF CONTROLLER DATA AND PROCESSING

1. The details regarding Controller Data and Processing are specified in Appendix 1.
2. The Processor shall not unreasonably withhold or delay its consent to amendments to Appendix 1.

3. CONTROLLER'S RIGHTS AND OBLIGATIONS

1. Controller is obliged to ensure that the Controller Data are Processed lawfully, fairly and in a transparent manner in accordance with the Regulation and National Law and has the corresponding rights.
2. Controller shall provide Processor with Instructions for Processing of Controller Data. Insofar, Controller has the comprehensive power to direct Processor as to the nature, extent as well as purpose and proceedings of the Processing of Controller Data.
3. During and after the term of this Agreement, the Controller is entitled to request from the Processor rectification, deletion, restriction of processing and transfer of Controller Data to the Controller.
4. The Controller may, upon prior notice, conduct an audit of the processing of the Controller Data carried out by the Processor, including, without limitation, verification of compliance with the implemented technical and organisational measures, in order to ensure that such processing is carried out in accordance with the provisions of this Agreement, the Controller's Instructions, the Regulation, and Applicable National Law. Unless a Personal Data Breach or other incident has occurred, such audit may be conducted no more than once per calendar year, during regular business hours and in a manner that does not disrupt the Processor's business operations.
5. Controller may exercise the right to audit the Processor on his own or authorize a representative to conduct the audit on his behalf. Processor shall allow and support any reasonable audit measures of the Controller or such representative (particularly, upon Controller's notification grant Controller or his representative access to his business premises and the relevant data processing devices and files where Controller data is processed).

4. PROCESSOR'S RIGHTS AND OBLIGATIONS

1. Processor shall Process Controller Data exclusively on behalf of and on the basis of Instructions of the Controller. Processor does not acquire any rights with respect to the Controller Data or other data derived therefrom.
2. The Processor shall not Process Controller Data in a manner that is incompatible with the initial purpose for which the Controller Data were collected, i.e. beyond the scope and purpose of Processing envisaged in this Agreement (in particular, as specified in Appendix 1) and the Master Agreement, including but not limited to the Processing of Controller Data for his own account. If in doubt, the Processor is obliged to obtain a written consent from the Controller before Processing the Controller Data.
3. Processing of Controller Data for purposes other than the ones described in this Agreement and the Master Agreement, including Processing of anonymized data, requires prior written consent from the Controller.
4. The Processor shall abide to all of the security measures defined by Controller for the duration of the processing and shall be responsible for any breach resulting from failure to comply with the stated measures.

5. TECHNICAL AND ORGANISATIONAL MEASURES

1. Processor guarantees that he has implemented appropriate technical and organisational measures in such a manner that the Processing meets the security and any other requirements for Processing of Controller Data set out in the Regulation (particularly those set out in Art 32), this Agreement and the Instructions, all in a manner which ensure protection of the data subject rights, including, by way of example, (i) encryption of data in transit (e.g. TLS) and, where applicable, encryption of data at rest; (ii) access control in accordance

with the principle of least privilege and the use of multi-factor authentication (MFA) for administrative and remote access; (iii) logging and monitoring of security-relevant events; (iv) vulnerability management and the application of security updates within reasonable timeframes; and (v) backups and recovery procedures in accordance with defined RPO/RTO parameters or agreed service levels (SLA). In particular, the Processor shall maintain during the term of this Agreement the technical and organisational measures as set out in Appendix 2. Appendix 2 shall be updated in case the standard or the technical or organisational measures change during the term of the Agreement.

2. In addition, the Processor guarantees that he has implemented such technical and organisational measures which enable the Processor to provide the Controller with any requested assistance regarding the Controller's obligations towards data subjects, supervising authority or any third party in relation to which Controller has statutory obligations.
3. Processor shall not make any copies of the Controller Data unless required to ensure proper Processing, provide the services under the Master Agreement, this Agreement or for the compliance with statutory retention obligations, the Regulation and/or National Law. Processor shall not disclose or transfer Controller Data to third parties unless authorized by Controller.

6. CONFIDENTIALITY

1. Processor shall oblige in writing all his employees and any other persons involved in Processing of Controller Data to abide by the obligation of ensuring confidentiality of the Controller Data. In doing so the Processor shall inform employees and any other persons involved in the Processing of Controller Data about the Regulation and National Law and the implemented security measures.
2. Processor shall record fulfilment of the obligation of confidentiality described in clause 6.1 in writing. Upon request of the Controller the Processor shall demonstrate to the Controller his compliance with such obligation by presenting to the Controller written employee declarations or other documentation of corresponding value.

7. INSTRUCTIONS AND ASSISTANCE

1. Processor is obliged to comply with the Instructions and requests of the Controller immediately upon receiving Instructions or requests from the Controller or, if any, within the reasonable deadline set by Controller.
2. Processor shall ensure that any employee or another person acting under the authority of the Processor, who has access to Controller Data, Processes the Controller Data only in accordance with the Instructions, unless he or she is required to do so by the provisions of the Regulation and/or National Law.
3. If in Processor's opinion the Controller's Instructions infringe mandatory provisions of the Regulation or National Law, Processor shall inform the Controller of the potential infringement prior to Processing the Controller Data. Upon Controller's confirmation he shall comply with the confirmed or amended Instruction.
4. Failure to inform the Controller on any Instructions that may infringe mandatory provisions, that the Processor was aware of, shall result in liability of the Processor.
5. Processor shall inform Controller immediately when Controller Data or other rights of the Controller are at risk due to attachment, seizure, insolvency proceedings or other events. Also, Processor will inform all relevant authorities in such events that the Controller Data and Controller's Data carriers are Controller's property. If Processor is subject to an information request regarding Controller Data he shall in due time before providing the information inform Controller about the recipient, time, and content of the information.
6. Where the Controller is obliged to provide information about Controller Data or any Processing activities in relation thereto, to a data subject, supervising

authority or a third party, the Processor shall provide the Controller, immediately upon receiving the request, with all the necessary information, documents or any other assistance required.

7. Controller shall designate an authorized person (including a substitute person) for communication the Instructions and requests, and Processor shall designate an authorized recipient (including a substitute person) to whom Instructions and requests shall be communicated. Changes in these designated persons shall be communicated to the other Party without undue delay. In urgent cases, Instructions and request may be communicated by and to other persons, if the designated persons are not available.
8. The Processor shall, taking into account the nature of the processing and the information available to the Processor, provide reasonable assistance to the Controller in fulfilling the Controller's obligations under Articles 35 and 36 of the Regulation (data protection impact assessment – DPIA and, where applicable, prior consultation with the supervisory authority), including by providing information on the technical and organisational measures and other relevant facts relating to the processing carried out by the Processor.
9. The Parties may agree that the assistance under this Article shall be provided within a reasonable scope and within time limits agreed in writing, and that assistance exceeding the customary scope of services may be subject to a separate fee.

8. RECORDING OBLIGATIONS

1. Processor shall maintain an electronic record of any Processing activities undertaken with regards to the Controller Data, within the meaning of maintaining records as defined in Art 30 (2) of the Regulation. It has to contain:
 - (a) the name and contact details of the Processor and Controller (including Controller's or Processor's representative, and the data protection officer, if any),
 - (b) the categories of Processing;
 - (c) where applicable, transfers of Controller Data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards, if required;
 - (d) a general description of the technical and organisational security measures.
2. Controller may request from the Processor a copy of the records on the Processing activities, which the Processor shall provide to the Controller immediately upon receiving the request.

9. PERSONAL DATA BREACH NOTIFICATION

1. Processor shall inform the Controller without undue delay if he discovers a Personal Data Breach or a potential Personal Data Breach, including, but not limited to a breach of this Agreement, Instructions, the Regulation or National Law by Processor or any of his employees.
2. The information on Personal Data Breach or a potential Personal Data Breach shall include information about the time and nature of the incident (including information about the data subjects and affected Controller Data, including an estimate on the number of affected data subjects and Controller Data), the affected system, the time of discovery, all potential consequences of the data-security-incident as well as the measure adopted or proposed by the Processor to address or mitigate the Personal Data Breach.
3. Initial notification to the Controller has to take place without undue delay after discovering the Personal Data Breach or a potential Personal Data Breach. Additional and more detailed notification containing all the relevant information regarding the Personal Data Breach as specified in clause 9.2

above has to be provided to the Controller within seven days from discovery of the Personal Data Breach or a potential Personal Data Breach.

4. Processor shall upon the Controller's first request and to any reasonable extent provide the Controller with any necessary or requested support relating to fulfilment of the statutory or other contractual obligations of the Controller with regards to the Personal Data Breach. Particularly, the Processor shall without undue delay adopt all reasonable measures to minimize and eliminate the threat for the integrity and confidentiality of the Controller Data, to secure the Controller Data and to prevent all potential negative consequences for data subjects or minimize their effects to the extent possible.
5. Processor shall perform and document a root cause analysis immediately after becoming aware of the Personal Data Breach and provide Controller with the documentation upon his request. If Controller determines that technical and organisational measures are inadequate, Processor shall implement at his costs appropriate technical and organisational measures in order to safeguard Controller Data against further Personal Data Breaches.

10. SUB-PROCESSING

1. Controller hereby gives the Processor a general authorisation to engage sub-processors for the Processing of Controller Data. The Processor shall inform the Controller in advance of any intended engagement or replacement of a sub-processor, thereby giving the Controller the opportunity to object on reasonable grounds related to data protection. If the Controller objects, the Parties shall discuss in good faith a feasible solution; failing that, the Processor shall not engage the relevant sub-processor for the Processing of Controller Data.
2. Where the Processor engages a sub-processor, the Processor shall impose on such sub-processor, by way of a written agreement, the same data protection obligations as set out in this Agreement (in particular those obligations referred to in Article 28 of the Regulation), including obligations relating to confidentiality, appropriate technical and organisational measures, assistance, and return or deletion of Controller Data, to the extent applicable to the sub-processor's services.
3. The Processor shall ensure that its sub-processing agreements clearly define the scope of the sub-processor's Processing, applicable security measures and responsibilities. The Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations and for any acts or omissions of the sub-processor that cause the Processor to be in breach of this Agreement.

11. TRANSFER OF CONTROLLER DATA

1. The Processor shall not transfer Controller Data to a third country or an international organization without obtaining previous written Instruction or approval of the Controller, unless required to do so for the purpose of complying with the Regulation or National Law.
2. In case of transferring Controller Data to a third country or an international organization for the purpose of complying with the Regulation or National Law, the Processor shall previously inform the Controller in writing of the intended transfer.
3. Obligation of requiring Controller's previous approval for transfer of Controller Data shall apply to any transfer of Controller Data to third parties, unless such transfer is envisaged in the Instructions.

12. DATA SUBJECTS RIGHTS

1. In case a data subject addresses the Processor directly, for the purpose of exercising the data subject rights (e.g. requests for access, rectification,

erasure, restriction etc of the Controller Data), the Processor shall without undue delay submit the request to the Controller. The Processor shall not engage in a direct request resolving, unless instructed otherwise by the Controller.

2. The Processor shall, immediately upon receiving such instruction from the Controller, comply with the instruction (e.g. rectify, erase, restrict etc the Controller Data). The documented record of the execution of the request shall be submitted to the Controller without undue delay.

13. LIABILITY

1. The Processor shall comply with the written instructions of the Controller and any material provision of this Agreement or the Master Agreement. The liability for the breach of this Agreement shall be subject to the statutory provisions on liability.

14. DURATION AND TERMINATION

1. Duration of this Agreement shall correspond to the duration of the Master Agreement.
2. This Agreement may be terminated under conditions envisaged for termination of the Master Agreement, as specified in the Master Agreement.
3. Controller may extraordinarily terminate this Agreement at any time for good cause. A good cause shall exist, in particular, if Processor:
 - (a) violates a material provision of this Agreement;
 - (b) uses Controller Data for other purposes than agreed in this Agreement.
4. In case of termination of this Agreement the Master Agreement shall only be continued if it can be excluded that Processor can Process or access Controller Data. In case of doubt the termination of the Master Agreement is deemed to also terminate this Agreement.

15. RETURN AND ERASURE OF CONTROLLER DATA

1. After the term of this Agreement, at the choice of the Controller, the Processor shall be obliged to delete or return all the Controller Data or other Personal Data generated therefrom to the Controller. This includes any existing copies thereof in Processor's possession, unless required differently by the Controller or National Law. Processor shall document in writing any deletion and destruction of Controller Data and provide Controller with such documentation upon his request.
2. The previous clause 15.1 also applies to any copies of Controller Data in all Processor's systems as well as for test data and garbage data, unless otherwise prescribed by the provisions of the Regulation and/or National Law.
3. Documentation evidencing the proper Processing of Controller Data in compliance with the Instructions, the Regulation and National Law shall be kept by Processor and shall be provided to Controller upon his request.

16. FINAL PROVISIONS

1. The Appendices form an integral part of this Agreement. In the case of discrepancies between provisions of this Agreement and provisions of the Master Agreement, the provisions of this Agreement with regard to data processing shall prevail.
2. Modifications of or amendments to the Agreement shall be valid only if made in writing and signed by both Parties, they must be expressly marked as such. This shall also apply to the present clause.
3. If any provision of this Agreement shall be declared invalid, illegal or unenforceable, such provision shall be severed and all remaining provisions shall continue in full force and effect and the invalid, illegal or unenforceable provision shall be deemed replaced by a valid and enforceable provision that

resembles the Party's intent regarding the invalid, illegal or unenforceable provision as closely as possible and is compliant with the Regulation and National Law. The same shall apply, mutatis mutandis, in case of an unintended gap in this Agreement.

4. This Agreement and any dispute or claim arising out of or in connection with it or its subject matter, whether of a contractual or non-contractual nature, shall be governed by, construed and enforced in accordance with the laws of the Republic of Croatia. Competent court is the court at the Processor's place of business.

APPENDIX 1

DETAILS OF PROCESSING

Subject-matter:	Processing of personal data related to the provision of services under the Master Agreement (support, administration)
Duration:	For the duration of the Master Agreement
Nature and Purpose:	Performance of obligations under the Master Agreement
Categories of Data Subjects:	Employees and external associates of the Controller
Type of Personal Data:	First name, last name, e-mail address, phone number
Data Location:	Controller's environment
Special Categories of Personal Data (if any):	None
Methods of Processing Personal Data (description of how the data are processed):	Access, entry, modification and deletion
Are cloud services used, and if so, which:	Yes (Microsoft cloud environment and Google cloud environment). NOTE: processing primarily takes place in the Controller's system.
If cloud services are used for data processing, specify the server location and whether data are transferred outside the EU/EEA:	The location is the EU; data are not transferred.
If data are transferred outside the EU/EEA, describe the protection mechanisms:	Not applicable
Are there any sub-processors (Microsoft, Oracle, etc.); if so, provide details:	Microsoft and Google. These processors have access to data when providing support.
Specify whether there are recipients of personal data other than sub-processors (pension funds, health funds, state authorities, etc.):	Not applicable.
Data flow diagram – high level is acceptable:	• Receiving the support request • Processing the minimum necessary data • Analysis and resolution, with controlled access to M365/Google

	• Escalation to the vendor, if needed, with minimum data
--	--

PROCESSOR CONTACT DETAILS: dpo@span.eu

CONTROLLER CONTACT DETAILS: Authorized contact person from the Master Agreement

DETAILS OF THE NATIONAL AUTHORITY (SUPERVISORY AUTHORITY):

Croatian Personal Data Protection Agency

Ul. Metela Ožegovića 16, 10000, Zagreb

Phone: 01 4609 000

APPENDIX 2

PROCESSORS TECHNICAL AND ORGANISATIONAL MEASURES

Measures for the Pseudonymisation and Encryption of Personal Data

Span has established a data classification process and, accordingly, defined data handling procedures based on data sensitivity. The information classification framework has been communicated to all employees, and additional training materials have been developed on this topic.

Span implements pseudonymisation and encryption measures in accordance with the results of risk assessments and the sensitivity of the data concerned.

Measures to Ensure Ongoing Confidentiality, Integrity, Availability and Resilience of Processing Systems and Services

Span is certified in accordance with the requirements of the international standards ISO/IEC 27001, ISO 22301, ISO 9001 and ISO/IEC 20000-1.

In line with these standards, Span has implemented organisational and technical security measures to ensure that:

- only the minimum amount of personal data necessary is processed; and
- appropriate technical safeguards are implemented and monitored on systems and databases based on risk assessment results.

Furthermore, in accordance with SLA requirements towards its customers, Span has identified key and critical applications/systems and defined availability and resilience scenarios accordingly.

Measures to Ensure the Ability to Restore Availability and Access to Personal Data in a Timely Manner in the Event of a Physical or Technical Incident

Span has identified key parameters (RPO and RTO) relating to data availability and acceptable data loss depending on business processes. Based on these parameters, backup and disaster recovery (DR) procedures have been defined.

In line with business needs, Span has implemented ISO 22301 (Business Continuity Management System framework) to establish, implement, maintain and continuously improve business continuity management processes.

Regular procedures are in place for testing, assessing and evaluating the effectiveness of technical and organisational measures ensuring processing security.

As part of its ISO compliance, Span conducts annual internal audits and undergoes external audits performed by independent third parties.

During both internal and external audits, testing and evaluation of the effectiveness of established technical and organisational measures are carried out. Successful completion of external audits is evidenced by ISO certificates published on Span's website.

Measures for User Identification and Authorisation

Each Span employee is assigned a named user account created within Active Directory (AD). Access rights are granted strictly on a least-privilege basis, depending on business needs.

Span operates a passwordless authentication model. Except in exceptional cases where connection to customer environments requires otherwise (in accordance with customer

requirements), authentication is performed using Microsoft Hello for Business with PIN or other methods defined by the controller's policies.

Where applicable, Multi-Factor Authentication (MFA) is implemented using Microsoft Authenticator for identity verification.

Measures for the Protection of Data During Transmission

Span uses secure encryption protocols to protect data in transit.

When connecting outside the corporate network, Span uses VPN and Microsoft DirectAccess, or other secure methods as defined by the controller's policies.

Sensitive data transmitted via email is encrypted. Encryption remains attached to the document, ensuring that only the intended recipient can open and read the email and its attachments.

When connecting to systems not operated by Span, Span aligns with the controller's security requirements and implements secure data exchange mechanisms accordingly.

Measures for the Protection of Data During Storage

Based on risk assessment results and data classification levels, appropriate technical protection measures (e.g., data encryption at rest) are implemented.

As a fundamental security measure, Span applies access control based on the principle of least privilege, thereby preventing unauthorised and/or excessive access to data.

Access to highly sensitive data is restricted strictly to individuals with a genuine business need. Microsoft Azure Information Protection (AIP) is configured accordingly to prevent unauthorised access to emails or documents classified at higher sensitivity levels.

Measures to Ensure Physical Security of Locations Where Personal Data Are Processed

Span ensures physical security at locations where personal data are processed.

Reception areas are staffed by Span personnel. Visitors are identified at reception and remain in the reception area until met by the relevant employee. Visitors are escorted at all times and supervised by responsible Span personnel.

Span employees access premises using contactless access cards. Higher-risk areas require additional access rights (e.g., server rooms, executive offices, HR, Legal, Finance and Accounting departments).

Where data are processed in data centres, Span conducts risk assessments of the respective provider and implemented security measures. Span relies on certifications and audit reports and processes data within Microsoft Azure data centres.

Measures to Ensure Event Logging

Identified critical and key devices are connected to a centralised logging system. The logging environment is centralised (SIEM and SOAR) and monitored by Span's Security Operations Centre (SOC) 24/7/365.

Automated processes are configured based on log events to notify responsible personnel and, where necessary, initiate blocking or other mitigation actions.

Measures to Ensure System Configuration, Including Default Configuration

Span performs regular system configuration backups to enable restoration in case of system failure.

Span follows industry best practices and implements system hardening measures wherever feasible, thereby reducing vulnerabilities across devices and the overall information system.

Measures for Internal IT Governance and IT Security Management

Span has established, documented and continuously improves processes relating to internal IT governance.

Span follows ITIL best practices and is aligned with ISO/IEC 27001 and ISO/IEC 20000-1 standards.

A Procedure for Handling Classified Data and Assets has been adopted, regulating the appropriate handling of information of varying confidentiality and integrity levels, as well as the proper handling of media containing such information, in order to prevent unauthorised disclosure, alteration and/or destruction.

Measures for Certification and Assurance of Processes and Products

In accordance with ISO 9001 requirements, Span has documented its processes and monitors, reviews and improves them as necessary.

Clearly defined and documented processes contribute to the quality of products and services delivered to customers.

Measures to Ensure Data Retention Limitation

Span maintains records of processing activities and has defined retention periods for personal data processing.

Retention periods are determined primarily based on applicable legal and regulatory requirements, followed by contractual obligations and internally defined retention schedules.

Measures to Ensure Accountability

Responsibilities are clearly defined in employment contracts. Additional details are provided in internal work regulations, while specific process-related obligations are described in separate policies and procedures accessible to all employees.

Regular training is conducted, and employees are informed of updates to internal acts, particularly those relating to personal data processing.

Span has appointed a Data Protection Officer (DPO) responsible for overseeing compliance with personal data protection requirements.

Privacy Rules have been adopted describing how personal data are collected, used and protected within Span. Data classification labels are defined to facilitate the identification and proper handling of sensitive information.

Employees are trained on appropriate conduct standards to reduce the risk of negligent handling of personal data.