Catre
Operatorii economici interesati

Ref: Invitatie depunere oferta

20.07.2021

Delgaz Grid SA
Achiziţii Adminsitrative

Andreea Campean

Mobil: 0724262255

andreea.campean@delgaz-grid.ro

Dear Sir / Madam,

Invitation for submitting an offer for concluding a contract for the implementation of a new service / functionality called WEBRTC for Delgaz Grid S.A.

1. The tender information

We hereby request for Delgaz Grid S.A. (DEGR) an offer for concluding a contract, having as object the implementation of a new service / features called WEBRTC (features that provide access for agents in the Call Center platform in tele-work conditions) necessary for the new technical set-up for Emergency Call Center.

We specify that the current remote access solution for call agents Center no longer meets group-level security requirements, exposing the company at a major security risk. Also supporting equipment the current solution no longer benefits from support and maintenance.

Implementation of a service / functionalities called WEBRTC for Call Center: The offer shall be structured as follows:

- Implementation services infrastructure and solution
- Annual maintenance subscription and support for the requested service

All the detailed specifications are in the attachement.

The contract will be concluded for a 36 months period.

The payment term accepted by DELGAZ GRID si 45 days EOM.

Might you have any questions feel free to send them until 22nd of July and the offer shall be submitted by 26th of July COB.

Cu stima,
Andreea Campean

Global Category Manager IT

Web Remote agents access solution for Delgaz Grid S.A. call center

A. **As IS description**:

Delgaz Grid S.A.(DEGR) has in place a call center solution based on Aspect Unified IP. Below a high-level architecture.

B. **Necessity**:

According with the actual pandemic context DEGR is looking after a web remote access solution for call center agents. The solution main characteristics must be:

1. Possibility to be adapted within Microsoft Azure Cloud environment.
2. To be adaptable according with best practice in regards with information security.
3. To be scalable up to 100 remote agents.
4. To be accessible via web browser and support remote agent login for the Aspect Unified IP call center
5. To be scalable and adaptable for high-availability and/or disaster recovery scenario

C. Technical requirements:

Related groups of agents that will access the isolated Aspect Unified IP call center (contact center), must have a secure and reliable means to connect with the systems and handle voice interactions.

Technical design should cover the expressed and implied requirements with a solution based on standard WebRTC technology.

The solution should have the capability to be connected with more than one Aspect Unified IP contact centers and more than one CRMs from the one installation.

The solution should have multi-tier architecture.

During normal operations, agents will connect to the web server that are serving the Unified IP they are logged in. In case of failure of any web server, or process, then the agents should be able to connect to the web servers of the other site for logging-in the Aspect Unified IP.

With this Active-Active deployment mode there should be adapted benefits like:

1. Zero down time upgrades for any component of the middleware itself
2. Zero down time for any upgrades of the Agent Web Portals of the contact center
3. Advanced capabilities for integrating one or more CRM from the same solution installation in the future
4. Omni-channel capabilities as Web Toolbar to be able to deliver all digital channel interactions like social, mail, Video, Web Chat, and Web Collaboration.

D. Offer presentation:

a. Hardware & Software Requirements

Hardware		
CPU		
RAM		
HDD Storage		
Network		
Software		
Operating System		
Services		
Other Services		

b. Commercial model: SAAS (pay as you go) for 3 years and one-off costs for professional services

Software Licenses

DESCRIPTION	QUANTITY	UNIT PRICE (€)	TOTAL (€)
	60		

Professional Services

DESCRIPTION	QUANTITY	UNIT PRICE (€)	TOTAL (€)

Information Security Requirements & Technical and organizational measures for Data Protection

Protection Level HIGH / VERY HIGH

The technical and organizational measures outlined here are agreed between _____

(complete company name CLIENT) and

_____ (complete company name SUPPLIER).

1 Information Security Requirements

Global Requirements are requirements which generally apply to the provision of all Services by SUPPLIER.

1.1 Reputable Sources

SUPPLIER ensures that hardware and software products are obtained from known and reputable sources, and that there is reliable technical support and a traceable supply chain.

1.2 Security Governance

SUPPLIER establishes, maintains and monitors an information security governance framework, which enables SUPPLIERs' governing body to set clear direction for, and demonstrate their commitment to, information security and risk management.

1.3 Information Risk Management

SUPPLIER ensures that (i) prior to implementing new IT environments which host information of the CLIENT including personal data (hereinafter referred to as „CLIENT information"), (ii) prior to implementing major changes to existing ones, and (iii) introducing significant new technologies, the associated information security risks are identified, evaluated, treated, monitored and kept within acceptable limits. The information related to risk management activities is shared with the CLIENT on request without undue delay.

1.4 Security Management

SUPPLIER has (i) established a specialist information security function, led by a sufficiently senior manager, which is assigned adequate authority and resources to ensure that good practice for information security is applied effectively and consistently throughout the company and that compliance with legal, regulatory and contractual requirements affecting information security is ensured. SUPPLIER (ii) maintains a comprehensive, ongoing security awareness program, to promote and embed expected security behavior in all individuals who have access to CLIENT information.

1.5 Documented Operating Procedures

SUPPLIER has established responsibilities and procedures for managing and operating its Services to ensure such documentation is (i) in line with recognized industry standards and best practices, (ii) properly documented in writing and (iii) up to date at all times during the Term of this Agreement. The operating procedures documentation shall be shared with the CLIENT on request without undue delay.

1.6 Asset management

SUPPLIER ensures that (i) assets (hardware and software, hereinafter referred to as „assets") which are used to create, process, store or transmit CLIENT information are protected against corruption, loss, theft, and unauthorized disclosure throughout their life cycle. SUPPLIER ensures that these assets are recorded in a register which is (ii) protected against unauthorized change, (iii) kept up-to-date, (iv) backed up regularly and (v) contains

necessary details about assets and include – if applicable – compliance requirements related to assets. SUPPLIER ensures that (vi) all assets are assigned to an owner who is responsible for the operation of the asset.

1.7 Physical Security

SUPPLIER must take appropriate precautions for physical security and access protection. In particular, measures must be implemented for protection against fire and water, protection against or avoidance of extreme temperatures (air conditioning), emergency power supply. Access to areas with information or systems that process CLIENT information or support processes that affect the security of CLIENT information must be restricted to an authorised group of persons (least privilege). This also includes access protection measures for data centers, including monitoring of critical areas, access logs, access by external company employees only if accompanied and security measures against intrusion.

1.8 System access

SUPPLIER restricts access to assets where CLIENT information is being created, processed, stored or transmitted to authorized individuals for specific business purposes. This includes at least that (i) only authorized users can gain access to CLIENT information, (ii) access privileges are limited to approved system functionality, (iii) there is appropriate segregation of duties, (iv) access privileges are not being assigned collectively (User IDs and passwords may not be shared). SUPPLIER ensures that administrative access to systems which store or process CLIENT Information is (v) restricted to minimal number of administrators, (vi) protected by 2-factor authentication procedure or where 2-factor authentication is technically not possible, equivalent security (such as temporary generated passwords in management systems). SUPPLIER further ensures that administrative access is (vii) always logged to enable detection and investigation of unauthorized access to and unauthorized manipulation of CLIENT Information. (viii) Furthermore, SUPPLIER ensures that a formal procedure is in place and maintained which describes how roles, accounts, access rights and privileges regarding administrative access are created, regularly reviewed, modified, locked and deleted.

1.9 System Management

SUPPLIER operates systems which create, store, process or transmit CLIENT information to (i) cope with current and predicted workloads and (ii) configures them in a consistent, accurate manner to protect them, and the CLIENT information they process, store or transmit against malfunction, cyber-attack, unauthorized disclosure, corruption, theft and loss. SUPPLIER manages the security of systems by (iii) performing backups of essential information and software, (iv) applying a rigorous change management process and (v) monitoring against agreed service level agreements.

1.10 Network and Communications

SUPPLIER ensures to design physical, wireless and – if applicable – voice networks to (i) be reliable and resilient, (ii) prevent unauthorized access, (iii) use encrypted connections, and (iv) detect suspicious traffic. (v) SUPPLIER ensures to configure network devices (including routers, firewalls and wireless access points) to function as required and to prevent unauthorized and incorrect updates. SUPPLIER ensures to protect electronic communication systems by (vi) setting policy for their use, (vii) configuring security settings, (viii) hardening the supporting technical infrastructure. (ix) SUPPLIER ensures to conceal computer and network names and topologies from external parties. SUPPLIER ensures to restrict external access to information systems and networks by (x) establishing Demilitarized Zones (DMZs) between untrusted networks and internal networks, (xi) routing network traffic through firewalls or proxy firewalls, (xii) limiting the methods of connection to a required minimum, (xiii) granting access only to authorized business applications, information systems or specified parts of the network.

1.11 Technical Security Management

SUPPLIER installs malware protection solutions on systems where CLIENT information can be exposed to malware, including (i) servers (e.g. application servers, database servers, file servers, print servers, web servers), (ii) computing devices (e.g. desktop computers, laptops and other mobile devices) and (iii) office equipment (e.g. network printers, photocopiers, multifunction devices). (iv) Malware protection software should protect against all forms of malware (e.g. viruses, worms, Trojan horses, spyware, rootkits, botnet software, keystroke loggers, ransomware). (v) Malware protection software should be distributed automatically and within defined timescales. SUPPLIER ensures and regularly reviews that (vi) malware protection software has not been disabled or minimized in functionality, (vii) the configuration of malware protection software is correct, (viii) updates are applied correctly within defined timescales, (ix) scans are being performed on predetermined times, and (x) adequate notification of identified malware events is being provided.

1.12 Segregation of Test and Production Systems

SUPPLIER ensures that (i) test and production systems are at least logically isolated so as to reduce the risk of unauthorized access or unauthorized modification to productive systems. (ii) Should segregation not be possible, SUPPLIER ensures to establish specially modified procedures for the Change Request process and for dealing with incidents and emergencies to enable fast, appropriate responses to disruptions and problems on the productive systems. (iii) Productive data is not allowed in test or development environments and must be anonymized if containing personal data or personal identifiable data.

1.13 Software Development/Acquisition

SUPPLIER ensures that internally developed software or externally acquired software, which is used to process, store or transmit CLIENT Information, is not vulnerable with regards to "OWASP TOP Ten" and "SANS Top 25 Most Dangerous Software Errors".

1.14 Vulnerability Scanning

SUPPLIER ensures that (i) systems are regularly (at least monthly) tested against vulnerabilities and configuration failures by performing dynamic tests (penetration test or vulnerability scans). (ii) All findings of such tests relevant to the CLIENT are shared with the CLIENT without undue delay; (iii) critical vulnerabilities shall be reported to the CLIENT immediately. (iv) SUPPLIER provides assistance and support for security patch and vulnerability management audits conducted by the CLIENT. (v) Mitigation of security vulnerabilities shall be performed based on their risk level and corresponding time frames agreed between the Parties.

1.15 Up-to-date Patch Levels

SUPPLIER ensures to remediate technical vulnerabilities by operating a patch management process which ensures to (i) identify and obtain patches from authorized sources, as soon as they are available, (ii) to decide when to deploy patches, (iii) test patches against a known criteria, (iv) deploy patches in a timely manner, (v) record patches that have been applied in a CMDB. (v) SUPPLIER is empowered to apply patches in the IT environment, including virtualization hypervisors, virtual machines, operating systems, and Applications as long as this does not have a negative impact on confidentiality, integrity or availability of CLIENT Information.

1.16 Minimum Credential Requirements

SUPPLIER ensures that CLIENTs minimum requirements for credentials (Two-factor authentication) are enforced via CLIENT federated Single-Sign-On solution for the IT environment operated to store or process CLIENT Information. The principle of least privileges and need to know and Segregation of duties must apply. Furthermore a Role Based Access Control design must be applied.

1.17 Network Design Requirements

There must be a multi-tier architecture and a DMZ for applications that are accessible from the Internet. Network segments must be segregated from segments for low and medium levels with appropriate security measures to prevent data traffic between the segments. The network segment for the very high level should preferably also be segregated and secured from the segments for the high levels.

1.18 Remote access and mobile working

SUPPLIER shall ensure that remote access possibilities are protected according to the current state of the art. Mobile working of SUPPLIER's employees with access to CLIENT information must be notified to the CLIENT in advance (as a general fact, but not for individual employees) and may only take place under the condition that the employees have been trained and committed in writing to comply with data protection and operational regulations. The SUPPLIER shall provide its employees with software and hardware for this purpose, which may only be used for business purposes or which supports an effective separation of business and private data (e.g. container solutions). Confidential documents are to be kept safe from access by third parties; documents may only be disposed of on the SUPPLIER's premises within the framework of disposal/destruction in accordance with data protection regulations. The agreed security measures must also be observed when providing the service in mobile work. Listening in and reading by unauthorized persons must be excluded. The SUPPLIER shall provide the Client on request with all information necessary to prove compliance with the specifications for mobile work.

1.19 Encryption

Data-at-Rest and Data-in-Motion (in-Transit) shall only be stored and transmitted using secure protocols and state-of-the-art encryption. Authentication features (passwords, PINs) may only be transmitted encrypted over the network. In addition, physical transports of storage media must be secured by physical protection and encryption.

1.20 Hardening

All information and network systems must be hardened. This includes (i) disabling of unnecessary applications, services, tools, protocols and interfaces, (ii) deleting or at least changing of vendor-supplied default user names and passwords, (iii) activation of security enhancing options and (iv) prevention of transfer of technical information to external entities.

1.21 Availability and Support

Unless otherwise agreed between the parties, SUPPLIER ensures the following requirements regarding availability, support, RPO and RTO are realized:

- availability of 99.6% or higher
- 24/7 support
- Recovery Point Objective (RPO) < 8 hours
- Recovery Time Objective (RTO) < 24 hours

1.22 Security Event Logging

To enable detection and investigation of unauthorized access to and unauthorized manipulation of CLIENT Information, SUPPLIER ensures that (i) event logging is enabled at all times for all systems operated by SUPPLIER to create, store, process or transmit CLIENT Information, (ii) systems are configured to generate security-related events and events with relevance for data integrity (including event types such as changes to CLIENT information, successful and failed user login attempts, service creation/modification/ deletion, object

creation/modification/deletion, system crashes, deletion of user accounts) and event attributes associated with each event (e.g. date, time, UserID, filename and IP address), (iii) consistent, trusted date and time sources ensure that event logs use accurate time-stamps (e.g. by using NTP servers), (iv) security-related event logs and event logs with relevance for data integrity are protected from unauthorized access and accidental or deliberate modification/overwriting, (v) security event logs are being extracted to a central store operated by CLIENT in real-time. For this purpose both Parties agree to jointly define and implement a concept which details how the event logs will be extracted and agree to jointly maintain this concept throughout the provision of Services in order to ensure that changes to the IT environment do not impact the availability of event logs or use cases for security event management. (vi) In addition, SUPPLIER ensures that any kind of forensic analysis/activities affecting systems which create, store, process or transmit CLIENT Information is being carried out together with an CLIENT IT Security staff member in order to satisfy a four-eye principle if requested.

1.23 Compliance Management

SUPPLIER ensures that (i) all systems which create, store, process or transmit CLIENT Information are regularly scanned for compliance with SUPPLIER's own "Security Policies/Standards". (ii) SUPPLIERs own "Security Policies/Standards" must be mapped and in-line with the certificates stated in Sections 2 & 3 of this Schedule. (iii) Compliance reports to prove such technical compliance checks for each IT asset within the IT environment are being provided to the CLIENT on request. Compliance reports must include a mapping between the related controls resulting from Sections 2 & 3 of this Schedule and the technical compliance check. (iv) The "Security Policies/Standards" of SUPPLIER are shared with the CLIENT prior to the Effective Date and upon request made by CLIENT thereafter.

1.24 Secure Disposal and Re-Use

SUPPLIER ensures that hardware to be decommissioned is (i) either sanitized prior to being re-used, sold or returned such that all CLIENT Information is securely erased in its entirety (ii) or is securely destroyed. (iii) Sanitization or destruction shall be performed in a secure way using state of the art technology and practices, such as tools and practices defined in NIST 800-88 "Guidelines for Media Sanitization". (iv) The concepts for secure disposal and deletion as well as evidence for secure disposal and deletion of CLIENT information assets are shared with the CLIENT on request.

1.25 Human Resources Security

For every individual acting on behalf of the SUPPLIER and granted access permissions (locally or remotely), personal identification information has to be made available to the CLIENT. SUPPLIER ensures an in-person identity proofing for human entities and that no one misuses access or permissions granted to individuals by SUPPLIER. SUPPLIER shall ensure that the authorizations granted are immediately withdrawn after termination or change of persons and/or responsibilities. Furthermore the SUPPLIER takes the responsibility for any occurred damages through unauthorized access and/ or use of CLIENT Information. The SUPPLIER only commissions personnel, which is demonstrably qualified for the necessary tasks.

1.26 Supply Chain Security

SUPPLIER ensures to identify and manage information risk throughout each stage of relationships with external SUPPLIERs of hardware and software throughout the supply chain by (i) embedding information security requirements in formal contracts and (ii) obtaining assurance they are met. (iii) SUPPLIER ensures that subcontractors involved in the processing, storing, transmission or disposal of CLIENT information at least meet the requirements agreed in this Schedule. (iv) The SUPPLIER is responsible for ensuring an appropriate governance of the Subcontractor/s as well as for the compliance of outsourced controls.

2 Data Protection Requirements

2.1 Commitment to confidentiality

SUPPLIER shall obligate all employees who process personal data of the CLIENT or have access to such data in writing to maintain confidentiality with respect to the handling of personal data.

The SUPPLIER shall train all employees who process personal data of the CLIENT or have access to such data with respect to data security and data protection. Participation will be documented on a name specific basis.

2.2 Data Protection by Design

SUPPLIER shall make regulations on "Data Protection by Design" in order to consider the right to data protection in the development and design of products, services and applications (e.g. by measures such as data minimization, pseudonymization, data protection-friendly default settings).

2.3 Data protection officer

In accordance with the legal requirements (Article 37 to 39 GDPR and national law), a data protection officer is designated.

Data protection officers shall have no conflict of interests.

The data protection officer possesses the qualifications and reliability required for the specific company.

The management supports the data protection officer.

The data protection officer is directly subordinated to the management and reports directly to it.

The data protection officer is informed and involved in the planning of new processes or the modification of existing processes on a timely basis.

The data protection officer actively participates in process design.

2.4 Data protection management system

SUPPLIER has established a data protection management system which meets the requirements of the GDPR and is subject to a continuous testing and improvement process.

With regard to the processing of personal data, risk analysis is conducted based on established and transparent criteria, and information security and data protection risks are identified, evaluated and properly handled in a compulsorily established and continuous process based on these criteria, and the effectiveness of the measures is reviewed by regular internal audits.

A data protection report is issued quarterly regarding the current status of the effectiveness of the data protection management system and any failures or data protection/security relevant events, and is made available upon request.

The management is fully informed and integrated in an information security and data protection organization and the respective communication, escalation and decision processes and ensures that the tasks and responsibilities can be executed to the extent required and with satisfactory quality.

Sufficient resources are made available for establishing, implementing, executing, monitoring, reviewing, maintaining and improving the data management system, and proof of the availability exists.

It is guaranteed that only personnel that have sufficient skills to comprehend the assigned tasks are involved in operating the data protection management system. This is ensured by instruction and other training measures.

Internal audits regarding data protection statuses are conducted on a regular - at least annual - basis, independent of IT security and risk evaluations. This makes it possible to recognize variations between the contractually established data protection level (all of the agreed technical and organizational measures, TOMs) and the actual data protection status, which than can be evaluated with regard to the resultant risk and provided on request.

A plan of action is established after data protection management audits that clearly states with which steps and within what appropriate time frame the established deltas are removed. This can be made available on request.

Continuous improvement of the Data Protection Management System is based on the Plan-Do-Check-Act Cycle, under which the principal becomes aware on request of the Plan phase and is involved in the execution (Act) if dedicated and multi-client resources are involved in the personal data of the principal.

The Data Protection Management System is tested for effectiveness by internal and external (inspection) testing.

3 Certifications

SUPPLIER agrees to maintain the following certifications:

- ISO/IEC 27001: All data hosting and support facilities where CLIENT Information is stored or processed are certified in accordance with ISO/IEC 27001 “Information Technology – Security Techniques – Information Security Management Systems – Requirements”.

SUPPLIER agrees to share the respective certificate as well as the “Statement of Applicability” with the CLIENT prior to the Effective Date, upon its renewal and according requests made by the CLIENT at any time during the Term of this Agreement.

SUPPLIER agrees to ensure that the “Statement of Applicability” covers all hosting and operations facilities, Applications and processes where CLIENT Information is processed or stored.

4 IT Security Process Interfaces

Both Parties agree to announce and provide contact persons for the following IT Security processes:

- Compliance Management: To exchange information regarding compliance with the requirements, provide certificates and reports as defined in this Schedule on an ongoing basis and to discuss and agree on actions to treat existing non-compliances and related risks. Truthful answers to the questions of the "supplier self-assessment" via the CLIENT risk management platform.
- IT Security Incident Management and personal data breaches: To exchange information regarding IT security incidents or IT security events that could result in an IT security incident that affects or could affect the IT environment operated to store or process CLIENT Information. “IT Security Incident Management” also includes the management of requests issued by the CLIENT for forensic analysis. Personal data breaches, and IT security incidents with data protection relevance must be reported by the SUPPLIER to the CLIENT immediately, but at least within the legally prescribed deadline; in this respect, reference is made to the relevant provisions of the data protection agreement.
- Risk Management: To exchange information regarding the risk management activities performed by SUPPLIER to ensure information security risks are appropriately identified, evaluated, treated, monitored and kept within acceptable limits on an ongoing basis.
- Vulnerability Management: To exchange information regarding vulnerabilities that affect or could affect the IT environment operated to store or process CLIENT Information and to discuss and agree on actions to mitigate existing vulnerabilities.

- Patch Management: To exchange information regarding the agreed maintenance windows and the roll-out of patches.
- Identity and Access Management: To exchange information regarding Identity and Access Management related topics.

Both Parties agree to jointly collaborate and exchange information within each of the above-mentioned security processes. The Parties shall agree on technical means to exchange information as well as Key Performance Indicators (KPI) to ensure the compliance to agreed security procedures.