msg.Check-In App – SaaS Agreement

Version 1.0 – 17.04.2023

value – inspired by people

msg.Check-In App

SaaS Agreement

between

**msg systems ag
Robert-Buerkle-Str. 1
85737 Ismaning**

GERMANY

– hereinafter referred to as “Provider” –

and

**<< Customer name >>
<< Street>>
<< ZIP Code >>**

<< COUNTRY >>

– hereinafter referred to as “Customer” –

conclude the following agreement (hereinafter referred to as “**Agreement**”):

§1 Subject of the Agreement

(1) The Provider renders SaaS services for the Customer using the Internet.

(2) Subject of this Agreement is the licensing of the software “msg.Check-In App” (hereinafter referred to as “SOFTWARE”) by means of an SaaS model, the use of the SOFTWARE via the Internet and corresponding SaaS services (hereinafter referred to as “SERVICE”) agreed upon in this Agreement.

(3) The Provider is entitled to involve subcontractors. The involvement of subcontractors does not release the Provider from his obligation to the Customer out of this Agreement.

§2 Provision of the SERVICE

(1) From the agreed date, the Provider provides the SERVICE, on the server infrastructure (hereinafter referred to as “SERVER”) made available by the Provider or its subcontractors, for the use according to these terms of this Agreement.

(2) The agreed functional scope of the SOFTWARE is described in Appendix 1 (User Manuel msg.CheckIn App).

(3) Customer access to the SERVICE is browser-based via the Internet or via an application interface set up by the Provider.

(4) For access and use of the SERVICE, the Provider will transmit the necessary access data, which is required for accessing the SERVICE, to the Customer.

(5) If a user account is required for the SERVICE, the Provider will provide this user account to the Customer once the agreement has been concluded. The creation of a user account is free of charge. The contractual relationship of the user account and the access data cannot be transferred. The Customer is liable for all actions taken under his user account.

(6) All passwords must be immediately changed by the Customer to passwords only known by him and must be kept strictly confidential. The Provider is not responsible for the consequences of misuse of user passwords.

(7) For the duration of this Agreement, the Provider shall hold available the Customer data transferred by the Customer to the SERVICE, which is necessary for the intended use of the SERVICE.

(8) Customer data is stored and regularly backed up by the Provider for the duration of this Agreement. It is the sole responsibility of the Customer to adhere to the Customer's trade and tax retention periods.

(9) The Provider shall eliminate software defects if technically possible. A defect exists if the SOFTWARE does not or not completely fulfill the functions specified in Overview | msg.Check-In (msgcheckin.com), delivers incorrect results or does not operate functionally so that the use of the SOFTWARE is impossible or limited.

(10) The Provider will continuously further develop and improve the SOFTWARE through updates and upgrades.

§3 Rights of Use of the SOFTWARE

(1) The Provider grants the Customer the non-exclusive, non-sublicensable and non-transferable right to use the SOFTWARE in accordance with the number of users specified in § 6 of this Agreement for the duration of the Agreement within the scope of the SERVICEs as intended.

(2) The Customer may only copy the SOFTWARE as far as this is covered by the intended use of the SOFTWARE according to the current service specification/User Manual.

(3) The Customer is not entitled to provide the SOFTWARE for use by third parties, neither in return for payment nor free of charge. Subletting the SOFTWARE by the Customer is hereby explicitly prohibited.

§4 Support / Service Level Agreement (SLA)

General Provisions

(1) This SLA specifies the availability of the supporting service levels. The Provider shall provide the services described below as of the date of conclusion of the Agreement.

(2) This SLA applies exclusively to the SERVICE provided to Customer for productive use and does not apply to non-productive, free and/or trial versions of the SERVICE and integration or test systems with unreleased features.

(3) All obligations of Provider in this SLA apply only to the SERVICE provided to Customer at the delivery point. The Provider is not responsible for data transmission from the delivery point to the Customer and/or in the area of the Customer's IT system.

Support

(4) The support includes a brief application consultation as well as a service desk for fault reports from the customer via the "Provide Feedback" button in the footer of the app or, if the app cannot be accessed, by e-mail to msg.Check-In@msg.group, prioritization of fault reports according to the urgency of the fault, analysis and rectification of the fault during the operating hours of the support.

(5) The Provider shall respond to inquiries of the Customer regarding the use of the SOFTWARE and the SERVICEs in accordance with the following Support operating hours:

Days	**Working Times:**	**Languages**
Monday to Friday, except on national holidays in Germany, as well as on 24.12. and 31.12.	9:00 to 17:00 CET (or CEST	German English

(6) All time information corresponds to the time valid in Germany (Central European Time (CET) or Central European Summer Time (CEST)).

Maintenance Works

(7) The Provider is entitled to interrupt the provision of the SERVICE for scheduled maintenance.

(8) The Provider will schedule maintenance work in such a way that the Customer's use of the SERVICE is affected as little as possible.

(9) Planned maintenance work is notified to the Customer at least 7 calendar days in advance.

(10) The Provider is also entitled to perform unscheduled maintenance of the SERVICE for good cause, e.g., if the service operation is endangered. This includes, in particular, emergency changes, e.g. the application of security patches, which are necessary to secure and maintain operations and require immediate implementation. The Customer must be notified immediately of such unscheduled maintenance work and it must be carried out in such a way that disruptions to the operating process are kept to a minimum.

(11) Adjustments, changes and additions to the contractual SERVICEs as well as measures serving to determine and remedy malfunctions will only lead to a temporary interruption or impairment of accessibility if this is absolutely necessary for technical reasons.

§5 Obligations of the Customer

(1) The Customer undertakes not to provide any data that is unlawful or violates laws, official requirements or the rights of third parties.

(2) The Customer is obliged to prevent unauthorized access of third parties to the protected areas of the SOFTWARE by taking appropriate precautions. In particular, the Customer shall, to the extent necessary, instruct its employees to comply with copyright law.

(3) Notwithstanding the Provider's obligation to back up data, the Customer itself is responsible for entering and maintaining its data and information required to use the SERVICEs.

(4) The Customer is obliged to check his data and information for viruses or other harmful components before entering them and to use state-of-the-art virus protection programs for this purpose.

(5) The Customer is provided with a "User ID" and password to access the use of the SERVICEs, which are required for further use of the SERVICEs. The Customer is obliged to keep "User ID" and password secret and not to make them accessible to third parties.

§6 Renumeration

(1) The Customer undertakes to pay to the Provider for the provision of the SOFTWARE and for the use of the SERVICEs under this Agreement a monthly fee according to the pricing information (plus statutory taxes) given in the aws marketplace.

(2) As soon as the limit for the price metric is exceeded, the monthly fee for the next higher category will be due starting with the next billing period. If the number of Users falls below the limit of the next lower category, the monthly fee of the next lower category will be due from the next billing period. In such cases, the Customer shall notify the Provider thereof by e-mail.

(3) Objections to the billing of services provided by the Provider must be raised by the Customer in writing to the office indicated on the invoice within a period of four weeks after receipt of the invoice. After the expiry of the afore mentioned period, the settlement shall be deemed approved by the Customer.

§7 Liability for Defects/Liability

(1) The Provider is liable for the functional and operational readiness of the SOFTWARE and the SERVICEs exclusively in accordance with the provisions of this Agreement.

(2) If the SERVICES are used by a non-authorized third party using the Customer’s access data, the Customer shall be liable for any accruing payments until the Provider receives the order by the Customer to change the access data and/or notification by the Customer about the loss or theft of access data.

(3) Provider is liable under the statutory provisions, without limitation

- for damage caused intentionally or negligently, due injury to life, body or health;
- due to the lack of warranted characteristics or non-compliance with warranty;
- for damages which are based on an intentional or grossly negligent breach of duty by the Provider.

Provider´s liability in all cases of contractual and non-contractual liability is limited to the contract typical foreseeable damages, which are based on a minor negligent breach of essential obligations by the Provider. Essential obligations within the meaning of this provision are obligations which enable the proper fulfilment of the Agreement in the first place and the observance whereon the Customer may rely. In all other cases, Provider´s liability for minor negligence is limited to an amount of 100.000,00 Euros. Subject to the provisions of the Product Liability Act, any strict liability of Provider is excluded.

§8 Data Protection/Secrecy

(1) Both parties will maintain data confidentiality and comply with data protection requirements in accordance with GDPR (General Data Protection Regulation). During the performance of the order, both parties shall only use the services of such agents or subcontractors who have been committed to data confidentiality and compliance with data protection requirements in accordance with GDPR and provide proof, if the other party so requires.

(2) Within the scope of this Agreement, the parties to the contract maintain silence about any information, which has to be treated as being confidential and/or to only use this information with third parties with prior written consent of the respective other party - regardless of the purpose. Information, which must be treated as being confidential are information provided by the disclosing party, explicitly designated as being confidential information or information obviously being of confidential nature.

(3) The obligations under § 8 (2) shall not apply to such information or parts thereof for which the receiving party proves that:

- the information has been known or has been publicly available before the date of receipt or information that has been rightfully received from a third party without breach of an obligation of confidentiality after the date of receipt; or
- the information has been known or has been publicly available before the date of receipt; or
- the information has become known or has become publicly available after the date of receipt without breach by the receiving party.

(4) Public announcements regarding the cooperation of the parties under this Agreement may only be pronounced subject to prior, mutual consent of the parties. The parties are not authorized to act as agents or trading partners of the other party. Without prior consent by the other party, neither party is entitled to use information about the intended or existing contractual cooperation for reference or marketing purposes.

(5) The obligations under §8 (2) shall continue to exist for an indefinite period of time beyond the end of the Agreement, and shall continue to exist for as long as an exceptional circumstance under §8 (3) is not proven.

(6) The terms and conditions of the Data Processing Agreement according to **Appendix 2** shall apply.

§9 Term and Period of Notice

(1) The Agreement enters into force upon signing. It has a minimum term of 1 month.

(2) After expiration of the minimum term or after each renewal period, the agreement is automatically renewed for another 1 month.

(3) The Agreement may be terminated by either party at the end of the minimum term or any renewal period by giving 30 days' written notice.

(4) The right of each contracting party to terminate the Agreement without notice for good cause shall remain unaffected. In particular, the Provider is entitled to terminate the agreement without notice if the Customer fails to make due payments despite a reminder and a grace period, or if the Customer violates the contractual provisions regarding the use of the SERVICEs.

§10 Applicable Law, Place of Jurisdiction

(1) This agreement shall be governed by the laws of Germany excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG).

(2) The exclusive place of jurisdiction for all disputes arising out of or in connection with this Agreement is Munich.

§11 Miscellaneous

(1) Ancillary agreements, amendments, additions hereto must be made in writing. This also applies to any waiver of the written form requirement.

(2) Should one or more provisions of this Agreement be or become fully or partially void or unenforceable then the validity of the remaining provisions shall remain unaffected. The invalid provision shall be deemed to be replaced by a valid provision that comes as close as possible to the economic purpose of the invalid provision. The same shall apply in the case of an unintentional gap in the provisions.

(3) Appendixes referred to in this Agreement form an integral part of this Agreement.

Signatures

msg systems AG

Ismaning, << Date>>

<< Name >> << Role / Position >>	<< Name >> << Role / Position >>

<< Customer >>

<< Location Customer >>, << Date >>

<< Name >> << Role / Position >>	<< Name >> << Role / Position >>

Attachments

Appendix 1: Data Processing Agreement msg systems

Appendix 2: TOM msg systems ag international 5.0

Appendix 1 - Data Processing Agreement

hereinafter referred to as "Contract" or "Order”

between

[Company]
[Street, House Number]
[Postcode]
[LOCATION]
- Controller –
hereinafter referred to as “Client”

and

msg systems ag
Robert-Buerkle-Strasse 1
85737 Ismaning
GERMANY
- Processor –
hereinafter referred to as “Supplier”

hereinafter jointly referred to as “the Parties”

The Supplier shall process the Client's personal data within the meaning of Article 4 No. 1 DS-GVO of the GDPR on the Client’s behalf. The Client shall be deemed to be the Controller, the Supplier shall be deemed to be the Processor within the meaning of the GDPR. Against this background, the Parties conclude the present data processing agreement pursuant to Article 28 of the GDPR.

1 Subject Matter and Duration of the Order

(1) Subject matter
The subject matter of the Order results from the msg.Check-In App – SaaS Agreement dated <<date>>, which is referred to here (hereinafter referred to as Main Contract).

(2) Duration
The duration of this order (term) corresponds to the term of the main contract.

(3) This contract shall apply without prejudice to the preceding paragraph for as long as the processes the Client's personal data (including backups).

(4) Insofar as other agreements between the Client and the Supplier result in other arrangements for the protection of personal data, this data processing contract shall take precedence, unless the parties expressly agree otherwise.

2 Specification of the Order Details

(1) Nature and Purpose of Processing of personal data by the Supplier for the Client are precisely defined in the main contract.

(2) Nature of the Personal Data

The Subject Matter of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories):

☒ Personal master data (key personal data)
☒ Contact data
☐ Key contract data (contractual/legal relationships, contractual or product interest)
☐ Customer history
☐ Contract billing and payments data
☐ Planning and control data
☐ Disclosed information (from third parties, e.g. credit reference agencies or from public directories)
☒ Check-In Information
☒ Team Allocation
☒ Follow-Following Relationships

(3) Categories of Data Subjects

The Categories of Data Subjects comprise:

☐ Customers
☐ Potential customers
☐ Subscribers
☒ Employees
☐ Suppliers
☐ Authorized agents
☐ Contact persons
☐ ……….

3 Technical and Organizational Measures

(1) The Supplier shall take all necessary technical and organizational measures in its area of responsibility in accordance with Article 32 of the GDPR for the protection of personal data and shall provide the Client with the documentation of these measures for review [Appendix 2]. Upon acceptance by the Client, the documented measures become the foundation of this contract.

(2) Insofar as the review/audit by the Client shows the need for amendments of the technical and organizational measures taken by the Supplier, this shall be mutually agreed between the Parties and subsequently implemented at the expense of the Supplier.

(3) The agreed technical and organizational measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. The Client shall be informed of any significant amendments which are to be documented by the Supplier.

(4) The Supplier is permitted to process personal data under this contract in private residences (home and teleworking).

4 Rectification, Restriction and Erasure of Personal Data

(1) The Supplier shall support the Client, within the Supplier's area of responsibility and as far as possible, by means of suitable technical and organizational measures in responding to and implementing requests from Data Subjects regarding their data protection rights. The Supplier may not disclose, port, rectify, erase or restrict the processing of personal data processed on its own authority, but only in accordance with the documented instructions of the Client.

Insofar as a Data Subject directly contacts the Supplier regarding their rights under Articles 15 - 21 of the GDPR (right to information, rectification, erasure, “being forgotten”, restriction of processing, data portability and objection), the Supplier shall forward this request to the Client.

(2) Insofar as included in the scope of services, the erasure policy, right to information, rectification, restriction of processing, erasure and data portability shall be directly ensured by the Supplier in accordance with documented instructions of the Client.

5 Quality Assurance and Other Duties of the Supplier

(1) In addition to complying with the provisions of this Order, the Supplier shall comply with the statutory requirements pursuant to the GDPR; accordingly, the Supplier shall, in particular, ensure compliance with the following requirements:

a) Written appointment of a Data Protection Officer, who performs their duties in compliance with Articles 38 and 39 of the GDPR.

- ☐ The Client shall be informed of the contact details of the Data Protection Officer for the purpose of direct contact. The Client shall be informed of any change of Data Protection Officer.
- ☐ Mr./Mrs. [Enter: first name, last name, organizational unit, telephone, e-mail] is appointed as Data Protection Officer at the Supplier. The Client shall be informed of any change of Data Protection Officer.
- ☒ The Supplier's current contact details are easily accessible on the supplier's homepage
- ☐ The Supplier is not obliged to appoint a Data Protection Officer. Mr./Mrs. [Enter: first name, last name, organizational unit, telephone, e-mail] shall be named as the contact person at the Supplier.
- ☐ As the Supplier is established outside the EU & EEA it designates the following Representative within the Union pursuant to Article 27 Paragraph 1 of the GDPR: [Enter: first name, last name, organizational unit, telephone, e-mail]

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Para. 4 of the GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who have authorized access to personal data, shall not process that personal data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) The Client and the Supplier shall, upon request, cooperate with the supervisory authority in performance of its tasks.

d) The Client shall be informed of any audits and measures conducted by the supervisory authority, insofar as they relate to this Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data under this Order.

e) Insofar as the Client is subject to an audit by the supervisory authority, an administrative or summary offense or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim or a request for information, in each case in connection with the processing of personal data under this Order with the Supplier, the Supplier shall make every effort to support the Client.

f) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the Data Subject.

g) Verifiability of the Technical and Organizational Measures conducted by the Client as part of the Client's supervisory powers referred to in Clause 8 of this contract.

h) The Supplier shall report breaches of personal data protection to the Client under this Order in such a way that the Client can fulfill its legal obligations, in particular pursuant to Articles 33, 34 of the GDPR. He shall prepare documentation on the entire process, which he shall make available to the Client for further measures.

i) The Supplier shall support the Client, within the Supplier's area of responsibility and to the extent possible, within the scope of existing information obligations vis-à-vis supervisory authorities and Data Subjects and shall provide the Client with all relevant information in this context.

j) Insofar as the Client is obligated to conduct a data protection impact assessment, the Supplier shall support the Client, taking into account the type of processing and the information available to him. The same shall apply to any existing obligation to consult the competent data protection supervisory authority.

(2) For the support services under Paragraph 1 above, the Supplier may claim remuneration for all expenses incurred in this connection.

(3) This contract does not release the Supplier from compliance with other requirements of the GDPR.

6 Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service in accordance with the main contract. This does not include ancillary services used by the Supplier, such as telecommunications services, postal/transport services, cleaning services or guarding services. Maintenance and testing services shall constitute subcontracting if they are provided for IT systems which are used to a significant extent for the provision of a service by the Supplier under the main contract. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's personal data, even in the case of outsourced ancillary services.

(2) The Supplier may only engage subcontractors (further Processors) with the prior express documented consent of the Client (at least in text form).

a) ☐ Subcontracting is not permitted.

b) ☒ The Client agrees to the commissioning of the following Subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 of the GDPR:

Company Subcontractor	Address/Country	Service	Information on appropriate safeguards Data transfer to a third country pursuant to Clause 7
msg systems ag	Robert-Buerkle-Str. 1 85737 Ismaning GERMANY	Provider of the Services according to the Main Contract	n/a
msg systems Romania SRL	Samuel Brassai 9 400104, Cluj Napoca ROMANIA	Processing of all Services according to Main Contract	n/a

c) ☐ The outsourcing to Subcontractors (if not specifically named in item b) as well as the outsourcing to Subcontractors other than those designated in item b) above

or

☐ the change of an existing Subcontractor

are permissible insofar as:

- the Supplier notifies the Client of such outsourcing to Subcontractors in advance in writing or in text form within a reasonable period of time, which may not be less than 10 days, and
- the Client does not object to the planned outsourcing in writing or in text form to the Contractor by the time of the transfer of the personal data and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of the Client's personal data to the Subcontractor and the Subcontractor's commencement of the data processing shall only be undertaken after compliance with all requirements for subcontracting has been achieved. Compliance with and implementation of the technical and organizational measures at the Subcontractor shall be checked by the supplier in advance of the processing of personal data, taking into account the risk at the Subcontractor, and then at regular intervals. The Supplier shall make the audit results available to the Client upon request. The Supplier shall ensure that the Client can also exercise its rights under this Agreement (in particular its audit rights) directly against the Subcontractors.

(4) The contractual agreement between the Supplier and the Subcontractor shall be submitted to the Client upon the latter's request, whereby business clauses not related to data protection law shall be exempt from the obligation to submit.

(5) If the Subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(6) Further outsourcing by the Subcontractor

☐ is not permitted;
☐ requires the express consent of the Main Client [designation] (at the minimum in text form);
☐ requires the express consent of the Main Supplier [designation] (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional Subcontractor.

7 International Data Transfers

(1) Any transfer of personal data to a third country or to an international organization requires a documented instruction from the Client and requires compliance with the requirements for the transfer of personal data to third countries in accordance with Chapter V of the GDPR.

☒ The provision of the contractually agreed data processing by the Supplier and any approved Subcontractors shall take place exclusively in a Member State of the European Union or in another State party to the Agreement on the European Economic Area.

☐ The provision of the contractually agreed data processing by the Supplier takes place in a third country with an adequacy decision pursuant to Article 45 of the GDPR.

☐ The Client permits a data transfer to a third country. Clause 6 Para. (2) b) specifies the measures to ensure an adequate level of protection from Article 44 et seq. of the GDPR in the context of subcontracting.

(2) Insofar as the Client instructs a transfer of data to third parties in a third country, the Client shall be responsible for compliance with Chapter V of the GDPR.

8 Supervisory Powers of the Client

(1) The Client shall be entitled to verify compliance with the obligations under this contract in consultation with the Supplier. The Client shall be entitled to carry out random checks, which must be notified in good time, at the Supplier's business premises during normal business hours. The Client shall be entitled to carry out inspections itself or to have them carried out by an inspector to be named by it in the individual case.

The Supplier is entitled to refuse the inspection by an auditor if the auditor is an employee of a competitor of the Supplier. The Supplier is at liberty to designate a different auditor.

The Client undertakes to keep confidential all information that becomes known to it in connection with such inspections. The Client shall also impose corresponding confidentiality obligations on the auditors it employs in individual cases.

(2) The Supplier shall ensure that the Client can satisfy itself of the Supplier's compliance with its obligations pursuant to Article 28 of the GDPR. The Supplier undertakes to provide the Client with the necessary information upon request and to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of the technical and organizational measures for compliance with the special requirements of data protection in general as well as those relating to this order can be provided by

☐ Compliance with approved Codes of Conduct pursuant to Article 40 of the GDPR;
☐ Certification according to an approved certification procedure in accordance with Article 42 of the GDPR;
☒ Current auditor’s certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor).
☒ A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the Federal Office for Security in Information Technology (BSI)).

(4) The Supplier may claim remuneration for all expenses that have been accrued to the Supplier in the course of enabling Client inspections.

9 Authority of the Client to Issue Instructions

(1) The Supplier shall process personal data only on the basis of documented instructions from the Client, unless it is obliged to process such data under the law of the Member State or under Union law. The Client shall confirm verbal instructions without undue delay (at least in text form). The initial instructions of the Client shall be determined by this contract.

(2) The Supplier shall inform the Client if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10 Deletion and Return of Personal Data

(1) Copies or duplicates of the personal data shall never be created without the knowledge of the Client. With the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as copies required to meet regulatory requirements to retain data.

(2) After completion of the contractually agreed work in accordance with the main contract or earlier upon request by the Client - at the latest upon termination of the main contract - the Supplier shall hand over to the Client all personal data that has come into its possession and that is directly related to the contractual relationship or, after prior consent, destroy it in accordance with data protection requirements. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

[Place],	[Place],
____________________	____________________
[Name] msg systems ag	[Name] [Supplement Client Name]
____________________	____________________
[Name] msg systems ag	[Name] [Supplement Client Name]

Appendix 2

TOM msg systems ag international 5.0

msg systems

.msg
.consulting
.solutions
.partnership
Automotive
Financial Services Food
Insurance Life Science & Healthcare Public
Sector Telecommunications & Media Travel & Logistics Utilities
Automotive Financial Services Food Insurance Life Science & Healthcare Public Sector
Telecommunications & Media Travel & Logistics Utilities Automotive Financial Services Food Insurance Life
Science & Healthcare Public Sector Telecommunications & Media Travel & Logistics Utilities Automotive Financial Services Food
Insurance Life Science & Healthcare Public Sector Travel & Logistics Utilities Automotive Financial Services Food Insurance Life Science & Healthcare
Travel & Logistics Utilities Automotive Financial Services Food Insurance Public Sector Telecommunications & Media Travel & Logistics Utilities
Automotive Financial Services Food Insurance Life Science & Healthcare Utilities communications & Media Travel & Logistics Utilities Automotive

Technical and organizational measures pursuant to Art. 32 EU-GDPR

Version:	5,0
As of:	March 2021
Classification:	intern

.consulting .solutions .partnership

.msg

1 Table of Contents

2 Generals

2.1 Objective and Purpose

Pursuant to Art. 28 Para. 3 c) in conjunction with Art. 32 Para. 1 GDPR, the data processor is to be carefully chosen in the context of the data processing agreement, with special consideration concerning the suitability of the technical and organizational measures taken by him. The technical and organizational measures described in this document according to Art. 32 GDPR are to be understood as msg standard and apply to all locations of msg systems ag. They shall apply between the parties provided that a data protection agreement has been concluded pursuant to Art. 28 GDPR. Individual supplements and details within the scope of the data processing are to be determined in the current data processing agreement.

2.2 Processing Notes by the Data Protection Officer

This document will be resubmitted for review or actualization in case of notifiable changes, but at the latest every year.

2.3 Declaration of Completeness, Release Declaration

The executive board of msg systems ag and the data protection officer confirm the completeness and correctness of the following information and hereby grant release for this document.

Ismaning, 8st March 2021

Dr. Stephan Frohnhoff
Digital unterschrieben von Dr. Stephan Frohnhoff
Datum: 2021.06.14 11:47:25 +02'00'

(Stephan Frohnhoff – CEO)

Rolf Kranz
Digitally signed by Rolf Kranz
Date: 2021.06.11 11:28:13 +02'00'

(Rolf Kranz – CSO)

Digital unterschrieben von Claus Bauer
Datum: 2021.05.31 10:49:40 +02'00'

(Claus Bauer – Data Protection Officer)

3 Infrastructure Information on msg systems ag

msg systems ag has a heterogeneous system landscape which is characterized by different server platforms and correspondingly supporting system software. The computer landscape includes Intel, IBM, HP and SUN servers with system software such as Microsoft Windows Server, Z/OS, Unix and Linux variants. The company uses standard market applications, databases and web tools for development, production, sales and support of its products.

An information security management system (ISMS) is gradually established at msg systems ag on the basis of the information security guideline that was approved by the msg board in 2016.

The initial certification of the ISMS according to ISO 27001:2013 took place in April 2017.

An existing TISAX Label is available for the locations in Ismaning, Stuttgart and Ingolstadt.

The central components of msg systems ag's IT infrastructure are delivered and operated by the central IT and Organization department.

Furthermore, cloud-based services are used within the scope of the msg cloud policy and restricted IT services are provided by external partners as part of multi-provider management. Examples of this are Office365 and other cloud service providers. In these cases, data protection agreements have been concluded with the service providers, insofar personal data is involved.

A cross-company security organization and regular meetings of the ISMS team with the data protection officer ensure the adequate consideration of the requirements of Art. 32 GDPR.

The main building of msg systems ag is located at Robert-Bürkle-Straße 1 in 85737 Ismaning (R1). The building is divided into different access zones. Depending on the authorization level, these zones can be entered via electronic access system with an access card or a transponder. The data center RZ1 is located in the main building. The data center RZ2 is situated at Max-von-Eyth-Straße 3 in 85737 Ismaning (E3). The backup data center is situated at Fraunhoferstraße 1 in 85737 Ismaning (F1).

The data centers are operated as FULL MANAGED DATA CENTER by the central IT and Organization department. Automated monitoring ensures 7 x 24 hours operation on 365 days. All three data centers are certified according to Tier 3+.

The structural design of the data centers includes

- Buildings made of solid reinforced concrete
- Architecture and statics: partial protection against debris load
- Fire-retardant exterior, extinguishing system with early fire detection
- Protection against ingress of extinguishing water, leakage sensors
- Raised floor with flexible ventilation control respectively InRow cooling systems
- Redundant air conditioning and ventilation systems
- Automated monitoring
- Security zones and access protection
- Video surveillance, alarm system and security service
- Emergency power supply units

4 Technical and Organizational Measures

At msg systems ag, compliance with and realization of the following measures are regulated by the information security guideline. These include policies for virus protection, Client-Security, network security as well as regulations for server and cloud use. msg systems ag operates an information security management system (ISMS) certified according to ISO 27001 and a quality management system (QMS) certified according to ISO 9001. A data protection management system (DPMS) takes into account the requirements of the GDPR and is structured according to the ISO 27701 model.

If further service providers are involved in the provision of services by the central IT and Organization department, they are also bound by data processing agreements. When selecting service providers, care must be taken to ensure that they are certified according to ISO 27001 or comparable certification standards.

A data protection officer is appointed to ensure the advisory and control functions within the framework of the GDPR and the BDSG. He is supported in his work by a data protection coordinator.

Contact details of the data protection officer: Mr. Claus Bauer, datenschutz@msg.group.

In addition to the provisions in the employment contract (obligation to confidentiality), employees receive data protection instructions at the beginning of their work. Later on, they are regularly sensitized through regular newsletters, trainings and personal contact.

The measures that ensure that the internal organization is designed to meet the requirements of data protection include:

- An ISMS/DPMS according to ISO 27001
- An existing TISAX Label is available for the locations in Ismaning, Stuttgart and Ingolstadt.
- An implemented ISMS-DB (Information Security Management System Database)
- A Corporate Security Management Portal
- An ISMS manual accessible to all employees
- An implemented CMDB (Configuration Management Database; description of IT components)
- Business Continuity Management (BCM) and Disaster Recovery procedures.
- A qualified Asset Management System

The protection goals, the confidentiality, integrity, availability and resilience according to Art. 32 GDPR are ensured by the ISMS/DPMS.

The measures pursuant to Art. 32 GDPR are described below.

4.1 Confidentiality

4.1.1 Physical Access Control

Measures to prevent unauthorized persons from accessing data processing equipment with which personal data are processed or used:

- Personalized, electronic access control systems for offices and data centers (multi-factor): Only authorized employees have access authorization. The corresponding access authorizations are checked regularly.
- Use of a transponder locking system for selected offices
- Instructions for handling access controls
- Guidelines for the company and identification of guests in the building
- Security by security service including regular patrols
- Depending on the location: use of alarm systems and data protection compliant video surveillance in security critical areas (e.g. data centers)
- Access lists in the data centers

4.1.2 Electronic Access Control

Measures to prevent data processing systems from being used by unauthorized persons:

- Organizational and technical regulations for the secure and proper use of passwords
- Server systems in the data centers can only be administered with a console password, further server systems can be administrated via password protected and encrypted connections
- Clear assignment of user accounts to specific users, no impersonal collective accounts
- Encryption of hard disks and data carriers, theft protection prescribed by security policy
- Use of multi-level protection mechanisms (multi-vendor virus scanners, multi-vendor firewalls)
- Use of a centrally controlled patch management and vulnerability management solution
- Guideline for physical protection of operating systems (Clean Desk Policy, screen lock, privacy filters)
- Network segmentation, network zones, firewalls
- Logical access control to the network, network access is granted only for approved corporate devices (certificate-based network access control solution)

4.1.3 Data Access Control

Measures to ensure that the persons authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, altered or removed without authorization during processing, use or after storage:

- Clean Desk Policy
- User identification and authorization approval procedures (identity and access management)
- Separation of authorization allocation (organizational) by the person responsible as well as authorization assignment (technical) by the IT department
- Use of an identity and access management platform
- Network drives with access only for authorized users / user groups
- Policy on the patch level of operational systems (Client-Security Policy)
- Through an independent access system in the data center

4.1.4 Separation Rule

Measures to ensure that data collected for different purposes will be processed separately:

- Logical and physical client separation
- The customer’s and other client’s data are processed, as far as possible, by different employees of the contractor
- Separation of test and production landscapes

4.1.5 Pseudonymization

Pseudonymization is a central technical and organizational security measure that the GDPR mentions not only in Art. 32 Para. 1 but repeatedly in various contexts. It can influence the lawfulness of the processing of personal data and increases the protection of the rights and freedoms of the data subjects. Recital 26 GDPR clearly states that even pseudonymized data still remain personal data.

Generally, three methods of pseudonymization are available:

- The data subject assigns a pseudonym himself and separates it from the data that identifies him.
- An independent third party who is in charge of the corresponding assignment rule assigns a pseudonym to the data subject (§ 7 Para. 1 Signature Act (SigG)).
- The responsible entity creates a pseudonym and separates it from the identifying characteristics of the data subject. Since the data processing entity itself is responsible for the assignment rule, such pseudonymization only offers protection against third parties. This procedure is stipulated in Recital 29 as a technical and organizational security measure.

The decision on the pseudonymization method depends on the particular use case. In the context of a data processing agreement, the pseudonymization is carried out by the controller so that the processor cannot identify the data subject without assistance of the controller.

4.2 Integrity

4.2.1 Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data media and that it is possible to check and establish to which entities personal data are to be transmitted via data transmission equipment:

- Security electronic transmission via encrypted connections (VPN, TLS)
- Security during transmission via secure file exchange platform (process description, logging)
- Security during physical transport (encryption of the data media, use of couriers)
- Documented data media destruction according to DIN 66399 for confidential and strictly confidential data

4.2.2 Input Control

Measures to ensure that it is possible to retroactively verify and identify whether and by whom personal data have been input, altered or removed from data processing systems:

- Only the employees of the contractor working in connection with services under the contract are authorized to process personal data of the client
- User authentication of persons authorized to enter, alter or delete data
- Authorization control of the access type (read or write access)
- Logging of the accesses

4.3 Availability and Resilience

4.3.1 Availability Control

Measures to ensure that personal data are protected against accidental destruction or loss:

- Backup and recovery concept with daily backup and storage of data media in separate fire compartments/data centers
- Procedure for restoring data from backups (e.g. restore only after an authorized request)
- Use of a central monitoring solution
- Use of a central SIEM solution
- Use of protection programs (virus scanner, firewalls)
- Use of a vulnerability management platform (server)
- Use of hard drive mirroring for servers and storage area (RAID)
- Use of uninterruptible power supply in the server area (USV, NEA)
- Use of air conditioning and fire protection (early fire detection, extinguishing system)

4.3.2 Resilience

Measures to ensure that personal data are protected in terms of robustness and resilience:

Incident/IT Service Continuity Management and Disaster Recovery Procedures (BCM)

4.4 Procedures for regular examination, assessment and evaluation

4.4.1 Order Control

Measures to ensure that personal data that on behalf of the client are only processed in accordance with the client's instructions:

- The respective contract with the client contains detailed information on the type and scope of the commissioned processing and use of the client's personal data, and specifies the authority to issue instructions
- The contract contains detailed information on the purpose of the use of the client's personal data, as well as a prohibition of use by the contractor beyond the written contract
- The contractor has appointed a data protection officer and ensures by the data protection organization that he or she is appropriately and effectively integrated into the relevant operational processes
- Documentation of IT service management activities (CMDB and ticket system)

4.4.2 Data Protection Management

A data protection management system ensures that accountability is maintained to demonstrate compliance with legal principles and regulations, the state of the art and the actuality and effectiveness of the measures. msg operates a data protection management system (DPMS) in accordance with ISO 27001, taking ISMS controls into account. The following measures ensure that an organization corresponding to the data protection regulations exists:

- Data protection organization with an appointed data protection officer in the msg group as well as appointed data protection coordinators in the entities
- Guidelines and instructions to ensure data protection compliance
- Obligation of the employees to maintain the data secrecy
- Regular data protection trainings for the employees
- Keeping a record of processing activities (Art. 30 GDPR) as a controller and processor
- Processes for safeguarding the rights of data subjects
- Audit of information security according to ISO 27001

4.4.3 Incident Response Management

The incident response management is documented and practiced within the ISMS and the DPMS at msg. Technical and organizational measures and processes ensure that detected or suspected security incidents are identified and systematically eliminated. Within the DMPS, a process ensures that a notification process is triggered in case of a personal data breach.

- Notification process for personal data breaches pursuant to Art. 4 No. 12 GDPR to supervisory authorities (Art. 33 GDPR)
- Notification process for personal data breaches pursuant to Art. 4 No. 12 GDPR to data subjects (Art. 34 GDPR)
- Notification process for personal data breaches pursuant to Art. 28 GDPR to the controller in the context of a data protection agreement

4.4.4 Privacy by Default

Appropriate technical and organizational measures ensure that processing is only carried out for the respective specific purpose with regard to the quantity, scope, storage period and accessibility by presetting.

The default settings are considered by msg in the context of standardized presets of systems and applications as well as the installation of data processing procedures.

Within the framework of privacy by design, functions and rights are designed and, regarding the data minimization, the lawfulness of certain inputs and input options (e.g. free text) is determined and decisions are made on the availability of data protection relevant usage functions (e. g. reporting).

The type and scope of the reference to persons as well as appropriate pseudonymization and anonymization are taken into account during project initialization.

When using our products, it is incumbent on you as a customer to ensure that your employees are informed about the proper use of our products and that data is processed exclusively within the scope of the specified purpose.

5 Document Overview

5.1 General provisions and copyright

5.2 Version History

Version	Description	Author	Date
3.0	Revision pursuant to GDPR	Claus Bauer	March 2018
4.0	Update	Claus Bauer	March 2020
5.0	Update	Claus Bauer	March 2021