Data Protection Annex GBS Cloud Services (“DPA”)

1 Preamble

The parties agree that this Data Protection Annex ("DPA") sets out their obligations with regard to the processing and security of Customer Data and Personal Data in connection with the services offered by the Provider. The DPA is incorporated by reference into the GTC GBS and the GTC GBS Cloud Services.

In the event of any conflict or inconsistency between these DPA Terms and other provisions in the Terms and Conditions, these DPA Terms shall prevail.

The Provider will comply with all laws and regulations that apply to the provision of its services, including data protection requirements. For the avoidance of doubt, The Provider is not responsible for compliance with any laws or regulations applicable to the Customer or the Customer's industry that are not generally applicable to the services that the Provider provides to the Customer. The Provider does not determine whether Customer Data contains information that is subject to certain laws or regulations.

Customer will comply with all laws and regulations applicable to its use of the Service, including but not limited to laws relating to confidentiality and data protection.

2 Definitions

Terms used but not defined in this DPA have the meanings specified in the Terms and Conditions . The following definitions have the following meanings:

"**Data Protection Requirements**" means the GDPR, local data protection laws and all applicable laws, regulations and other legal requirements relating to data protection and data security, as well as the use, collection, retention, storage, backup, disclosure, transfer, disposal and other types of processing of personal data.

"**Diagnostic Data**" means a specific type of data used in the investigation and diagnosis of IT system problems, transaction performance, errors, or erroneous output.

GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation).

"**Customer Data**" means all data, including but not limited to all text, sound, video or image files and software, provided to Provider by or on behalf of Customer through the use of the Service.

"**Local Data Protection Laws**" means all subordinate laws and regulations implementing the GDPR.

"**Personal data**" means any information relating to an identified or identifiable natural person.

An **identifiable natural person** is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more specific factors that express the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Service-generated data**" means data generated or derived by the Provider through the operation of an online service. Service-generated data does not include customer data, diagnostic data or data on professional services.

"**Standard Contractual Clauses**" are the standard data protection clauses for the transfer of personal data to processors in third countries that do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

"**Support Data**" means any data, including any text, sound, video, image or software, provided to Vendor by or on behalf of Customer (or which Customer authorizes Provider to obtain from an Online Service) through an agreement with Vendor to obtain technical support for Online Services covered by the Terms and Conditions.

"**Sub-processor"** means other processors involved by the Provider for the processing of Customer Data and Personal Data in accordance with Article 28 of the GDPR.

Any specific data protection provisions relating to the protection of personal data and used in this agreement have the meaning they have in the GDPR and other applicable data protection laws.

For the avoidance of doubt and as set forth above, data defined as Customer Data, Diagnostic Data and Service Generated Data may contain Personal Data.

3 Scope of the DPA

The conditions mentioned in this DPA apply to all services that the provider provides to the customer, as far as customer or personal data are concerned.

Previews may not cover the privacy and security measures specified for the Service. The customer may not use previews to process personal data or other data that is subject to legal or regulatory requirements.

4 Data protection regulations

4.1 Use of data and data processing

The Provider uses and processes Customer Data and Personal Data only in the name and on the instructions of the Customer in order to provide services and for the legitimate business operations of the Provider in connection with the delivery of the Services to the Customer to the extent described below. The customer reserves all rights, titles and interests to the customer data. The Provider does not acquire any rights to Customer Data, with the exception of the rights that the Customer grants to the Provider under this DPA. All instructions must be documented by the provider and presented to the customer on request. This paragraph does not affect the provider's rights to software or services that the provider licenses to the customer.

4.2 Processing for the provision of services

For the purposes of this DPA , the provision of the Service consists of:

- Secure customer communication.
- Search for malicious content; and
- Improve productivity.

In providing the Services, the Provider will not use or otherwise process Customer Data or Personal Data for user profiles, advertising or similar commercial purposes or market research, unless such use or processing is carried out in accordance with the Customer's instructions.

4.3 Disclosure of processed data

The Provider will not disclose or grant access to processed data except at the direction of the Customer, as described in this DPA or as required by law. For the purposes of this section, "processed data" means customer data, personal data and any other data processed by the provider in connection with the service and constituting confidential information of the customer. The processing of the processed data is subject to confidentiality in accordance with the general terms and conditions of the service.

The provider only passes on processed data to legal entities or grants them access to this data if this is required by law. If legally permissible, the provider will inform the customer about the respective request.

In the event that the Provider receives a request from a third party for processed data, the Provider will, where permitted by law, inform the Customer of the corresponding request.

In both cases and to the extent permitted by law, the Provider will attempt to direct the requests to the Customer. The provider is therefore permitted to provide the customer's contact information.

4.4 Roles and obligations of the parties

The parties agree that the customer, the controller of the personal data and the provider is the processor of the personal data. The Provider may use sub-processors to the extent described in Article 8 of this DPA. The provider will only process personal data to the extent that he has received documented instructions from the customer.

The Customer agrees that the Provider's Terms and Conditions (including the DPA Terms and Conditions current at that time and any applicable updates), together with the Product Documentation and the Customer's use and configuration of features in the Service, constitute the Customer's complete documented instructions to the Provider for the processing of Personal Data.

4.5 Obligations of the provider

The Provider is obliged to establish an internal organization for the protection of personal data that complies with the requirements of current legislation.

The Provider is obliged to take the technical and organizational measures that ensure the confidentiality, integrity, availability and resilience of the processing systems and services.

The Provider is obliged to establish a procedure for the regular review, assessment, and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing.

The Provider shall ensure that it implements all relevant technical and organizational measures in such a way as to comply with the requirements of the applicable legislation on the protection of personal data and, in particular, the protection of the rights of data subjects. Before the start of the processing, the Provider has set up the technical **Annex B – Technical and Organizational Measures (TOMs)** this DPA and will maintain them for the duration of this DPA.

The technical and organizational measures depend on the development of the technology. The Provider has the right to apply alternative reasonable measures that provide the same or a higher level of security.

As soon as it becomes aware of it, but no later than forty-eight (48) hours, the Provider will inform the Customer if a breach (or potential breach) of the Customer's personal data is detected. The Provider shall provide the sufficient information to enable the Customer to comply with its obligations to report a personal data breach to the supervisory authority. The Provider declares that it has created and implemented measures for the timely (if possible immediate) detection of breaches of the protection of the Customer's personal data, as well as for the traceability of the causes and consequences of the breaches.

The provider is obliged to immediately take all necessary and appropriate measures to remedy the breach of the security of personal data and to mitigate/prevent possible adverse consequences. The Provider shall inform the Customer as soon as possible of all measures taken by him.

Notifying Vendor of a security incident or responding to a security incident pursuant to this section does not constitute an acknowledgement of any error or liability of Vendor with respect to the security incident.

The Customer must immediately inform the Provider of any possible misuse of its accounts or authentication data or of any security incidents related to the Service.

Security Incident Notification(s) will be delivered to one or more of Customer's administrators by any means chosen by Vendor, including by email. It is customer's sole responsibility to ensure that customer's administrators provide correct contact information when logging in to each applicable online service portal and update it as necessary. Customer is solely responsible for complying with its obligations under the laws applicable to it regarding the notification of security incidents and the fulfillment of third-party notification obligations in connection with security incidents.

The provider is obliged to document any data protection violations that include the facts of the data protection violation in such a way that the customer can comply with the relevant legal reporting obligations (e.g. in accordance with Art. 33 and Art. 34 GDPR).

4.5.1 Obligations of the customer

The customer is obliged to give instructions to the provider due to the processing of the data before the date of acceptance of the General Terms and Conditions .

The Customer is solely responsible for making an independent decision as to whether the technical and organizational measures for the Service meet the Customer's requirements, including its security obligations in accordance with applicable data protection requirements. The Client acknowledges and agrees that (taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing of its personal data, as well as the risks to individuals), the security practices and policies implemented and maintained by the Provider provide a level of security appropriate to the risk in relation to its personal data. Customer is responsible for implementing and maintaining privacy and security measures for components it provides or controls.

If the Customer acts as a processor, the Customer guarantees that the instructions given by the Customer have been authorized by the respective controller.

4.6 Duration of processing

The processing will continue as long as the Provider provides services to the Customer on the basis of the General Terms and Conditions and in accordance with the Customer's instructions.

4.7 Rights of the data subject

If a data subject contacts the provider with the request to exercise his or her rights under the GDPR, the provider must immediately refer this data subject to the

customer. The provider has the right to respond to the request of the data subject only with the prior written consent of the customer. The Provider shall assist the Customer in processing a reasonable request to exercise the rights of the data subject.

The Provider undertakes, on the instructions of the Customer, to rectify, delete or block without undue delay the Customer's personal data relating to the data subject or to carry out any other appropriate measure requested by the Customer.

4.8 Request from the authorities

In the event that the Customer is obliged to provide information to a government authority on the processing of the Customer's personal data or otherwise cooperate with that authority, the Provider shall be obliged to assist the Customer in providing such information by assisting in the prompt provision of the relevant information or documentation, including: the technical and organizational measures taken, the places where the customer's personal data are processed and the persons involved in the processing.

5 Data transfer and location

5.1 Data transmission

The data processing activities are carried out on the territory of a Member State of the European Union (EU) or another Member State of the Agreement on the European Economic Area (EEA). Data processing in a country outside the EU may only take place if the special conditions of Chapter V of the GDPR are met.

5.2 Sub-processors

In the event that the Provider uses sub-processors who could transfer data, the Customer accepts the terms and conditions of the respective sub-processor regarding the data transfer.

6 Retention and deletion of data

The customer has the possibility to access, extract and delete the stored customer data at any time during the term of his subscription. After completion of the provision of the service, the provider is obliged, at the discretion of the customer, to return and delete all personal data provided by the customer and all additionally acquired personal data of the customer, including all copies, completely and irrevocably, unless and insofar as the exception pursuant to Art. 28 para. 3 lit. l. "g" of the GDPR.

The Provider creates a document for the deletion of the Customer's personal data and makes it available to the Customer. The customer may request the release of the corresponding log files at this time or at a later date.

The documentation, which serves to prove the conformity of the processing of the Customer's personal data with the service provided and the processing rules, will be kept by the Provider after the termination of the provision of services in accordance with the corresponding retention periods.

7 Confidentiality obligation of the data processor

The Provider shall ensure that its employees involved in the processing of Customer Data and Personal Data process such data only on the instructions of the Customer or as described in this DPA and are obliged to maintain the confidentiality and security of such data even after completion of the order. The Provider offers regular and mandatory data protection and security training and awareness-raising activities to its employees who have access to customer data and personal data in accordance with applicable data protection requirements and industry standards.

8 Use of sub-processors

The Provider may engage sub-processors to provide certain limited or additional services on its behalf. The Customer agrees to this assignment and the companies affiliated with the Provider as sub-processors by accepting the Provider's General Terms and Conditions.

The Provider provides information about sub-processors on a Website of the Provider. By accepting the General Terms and Conditions of the Provider, the Customer declares that he has read, understood, and accepted the respective data protection provisions of the sub-processors. When engaging a sub-processor, the Provider shall ensure that the Sub-Processor may only access and use Customer Data or Personal Data for the provision of the Services for which the Provider has retained it and that it is prohibited from using Customer Data or Personal Data for any other purpose. The provider is obliged to check compliance with the obligations at least once a year.

9 General Terms and Conditions

9.1 Limited Updates/Changes to DPA Terms

If Customer renews or purchases a new subscription to a Service provided by Provider, the then-current DPA Terms will apply and will not change during Customer's subscription to that Service. Notwithstanding the foregoing limitations on updates, as Vendor introduces new features, supplements, or related software, vendor may provide additional terms or make updates to the DPA that apply to Customer's use of them.

If these Terms contain material adverse changes to the DPA Terms, Provider will give Customer the choice to use the new features, supplements, or related software without losing the existing functionality of a generally available Service. If the customer does not use the new functions, additions or the associated software, the corresponding new conditions do not apply.

9.2 Legal regulations and requirements

Notwithstanding the foregoing limitations on updates, Provider may modify or terminate a Service in any country or jurisdiction where there is a present or future governmental requirement or obligation that subjects the Provider to a regulation or requirement that is not generally applicable to companies operating there that is a hardship for The Provider to continue operating the Online Service without modification and/or Leads Vendors to believe that the DPA Terms or the Service provided may conflict with such requirement or obligation.

9.3 Electronic notification

The Provider may send the Customer information and communications about the Service electronically, including by e-mail, in a way that identifies the Provider. Notifications shall be deemed to have been made on the day on which they are provided by the Provider.

9.4 Contact details of the provider

Der Kunde kann sich an den Kundensupport des Anbieters wenden unter:

support24@gbs.com

+49 69 808 852 88 (Hotline DE/EN 24/7/365)

10 Appendix A – Types of customer's data processed

This annex contains details on the processing of personal data pursuant to Article 28(3) GDPR.

10.1 Types of personal data:

- Name;
- PIN;
- Telephone number;
- Address;
- and so on.

10.2 Activities of **data processing**:

- Collecting;
- Record;
- Save;
- Forward;
- items;
- Delete;
- Destroy.

10.3 Purpose of processing:

- Secure customer communication.
- Search for malicious content.
- Comply with legal requirements by adding exclusion clauses.
- Improve productivity through out-of-office functionalities.

10.4 Categories of data subjects:

- employees.
- Customers.
- Contractual partners.
- Website visitors.

11 Annex B – Technical and Organizational Measures (TOMs)

11.1 Organizational security measures

11.1.1 Security Management

1) Security policy and procedures: The provider must document a security policy regarding the processing of personal data.
2) Rollen and responsibilities:
   a) The roles and responsibilities related to the processing of personal data are clearly defined and assigned in accordance with the Security Policy.
   b) In the case of internal restructuring or dismissal and change of employment relationship, the revocation of rights and obligations with appropriate transfer procedures is clearly defined.
3) Access control policy: Each role involved in the processing of personal data is assigned specific access control rights according to the need-to-know principle.
4) Resource/asset management: The provider has a register of IT resources used for the processing of personal data (hardware, software, and network). A specific person is responsible for maintaining and updating the register (e.g. IT officer).
5) Change management: The provider ensures that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). This process is regularly monitored.

11.1.2 Incident response and business continuity

1) Handling of incidents / personal data breaches:
   a) An incident response plan with detailed procedures will be established to ensure an effective and orderly response to incidents related to personal data.
   k) The Provider will immediately report to the Customer any security incident that has led to the loss, misuse or unauthorized acquisition of personal data.
2) Business continuity: The Provider establishes the main procedures and controls to be followed to ensure the necessary level of continuity and availability of the IT system in which personal data is processed (in the event of an incident/personal data breach).

11.2 Human resource management

1) Confidentiality of employees: The provider ensures that all employees are sufficiently informed and understand their responsibilities and obligations in connection with the processing of personal data. Roles and responsibilities are clearly communicated during the pre-hiring and/or induction process.
2) Training: The provider ensures that all employees are adequately informed about the security controls of the IT system that relate to their daily work. Employees involved in the processing of personal data shall also be adequately informed about the relevant data protection rules and legal obligations through regular awareness-raising campaigns.

12 Technical security measures

12.1 Pseudonymization

Customers' employees are encouraged to submit support requests with simulated/anonymized data - personal data of third parties is usually not available or is deleted.

12.2 Encryption

End-to-end drive encryption to customers and servers, encryption of all databases (server and customer side), encryption technologies for VPN connections.

12.3 Access control and authentication

l) An access control system is implemented that applies to all users who access the IT system. The system allows you to create, approve, review, and delete user accounts.
1) The use of shared user accounts is avoided. In cases where this is necessary, it ensures that all users of the shared account have the same roles and responsibilities.
2) When granting access or assigning user roles, the "need-to-know principle" must be observed in order to limit the number of users who have access to personal data to those who need it to achieve the processing purposes of the provider.
3) If the authentication mechanisms are based on passwords, the provider requires the password to be at least eight characters long and to comply with very strong password control parameters such as length, character complexity, and non-repeatability.
4) The authentication credentials (such as user ID and password) must never be transmitted unprotected over the network.

12.4 Logging and monitoring:

Log files are enabled for each system/application used to process personal data. They include all types of access to data (viewing, modifying, deleting).

12.5 Security of data at rest

12.5.1 Server/Database Security

a) Database and application servers are configured to run using a separate account with minimal operating system privileges to function correctly.
b) Database and application servers only process the personal data that is actually needed to achieve their processing purposes.

12.5.2 Security at Workplace:

a) Users are unable to disable or bypass security settings.
b) Antivirus applications and virus definitions are continuously updated.
c) Users do not have permission to install or activate unauthorized software applications.
d) The system has session timeouts if the user has not been active for a certain period of time.
e) Critical security updates released by the developer of the operating system are installed regularly.

12.6 Network/Communication Security:

1) Whenever access is via the Internet, communication is encrypted by cryptographic protocols.
2) Traffic to and from the IT system is monitored and controlled by firewalls and intrusion detection systems.

12.7 Back-ups:

1) Backup and data recovery procedures are defined, documented, and clearly linked to roles and responsibilities.
2) Backups receive an adequate level of physical and environmental protection that meets the standards applied to the original data.

3) The execution of the backups is monitored for completeness.

12.8 Mobile/Portable Devices:

1) Procedures for managing mobile and portable devices are defined and documented, which establish clear rules for their proper use.
2) Mobile devices that are allowed to access the information system are pre-registered and pre-authorized.

12.9 **Security in the lifecycle of applications:**

Throughout the development lifecycle, best practices, state-of-the-art and recognized safe development practices or standards are followed.

12.10 Deletion and destruction of data:

1) Software-based overwriting is carried out on media before they are disposed of. In cases where this is not possible (CD's, DVD's, etc.), physical destruction is carried out.
2) Paper and portable data carriers used to store personal data will be destroyed.

12.11 **Physical security**

The physical perimeter of the IT system infrastructure is not accessible to unauthorized personnel. Appropriate technical measures (e.g. intrusion detection system, chip card-controlled turnstile, one-person security access system, locking system) or organizational measures (e.g. security guard) must be taken to protect security areas and their access from unauthorized access.