

Supplementary Contractual Terms for Cloud Services - EVB-IT Cloud GTC –

1	Subject matter of the contract.....	2
2	Nature and scope of the services	3
3	Prohibitions of use	4
4	Place of performance.....	5
5	Access/storage space.....	5
6	Data protection, IT security and confidentiality	5
7	Data security service/backup/return and deletion entitlement	7
8	Availability	8
9	Reporting obligations	9
10	Disruption classification	9
11	Troubleshooting	10
12	Modification of the service after conclusion of the contract by the Contractor	10
13	Duties and performances in connection with the end of the contract.....	10
14	Rights of use	12
15	Subcontractor.....	13
16	Remuneration	14
17	Cooperation of the Principal	14
18	Rights of the Principal in the event of defects in the services	15
19	Limitation of liability.....	16
20	Term and termination.....	16
21	Liability insurance	16
22	Rights of retention and refusal of performance	17
23	Text form.....	17
24	Applicable law, place of jurisdiction	17
	Definitions	18

1 Subject matter of the contract

1.1 The subject matter of the contract is the services of the Contractor agreed therein.

The Contractor's services may in particular include:

- Software as a Service (SaaS)*,
-
- Platform as a Service (PaaS)*,
- Infrastructure as a Service (IaaS)*,
- Managed Cloud Services (MCS)*,
- Other services related to the aforementioned services, such as initial services.

Insofar as the Contractor processes and/or hosts data of the Principal when providing services on behalf of the Principal, this shall be part of the services due.

1.2 The Contractor shall provide the services in compliance with the Cloud Computing Compliance Criteria Catalogue - C5 (Basic Criteria) current at the time of conclusion of the contract. In addition, the Contractor shall observe the security requirements made part of the contract by the Principal, e.g., from its security guideline in terms of the minimum standard(s) of the Federal Office for Information Security (BSI) for the use of external cloud services.

If the C5 catalogue of requirements (basic criteria) changes during the term of the contract, the Contractor shall endeavour to meet the new or changed requirements within a reasonable period of time. If the Contractor does not declare to the Principal upon request within twelve months (subject to another implementation period specified by the legislator, which must be observed in any case) from the publication of the successor document that it fulfils the new and amended requirements, the Principal shall have a special right of termination with respect to the affected services to be exercised with a notice period of one month. The Principal shall not lose the special right of termination by not exercising it immediately. The renewal of any test certificates shall take place in the usual test cycle.

1.3 The Contractor shall be obliged to monitor its performance continuously by suitable technical means (monitoring*). The reporting obligation from clause 9 is not extended by this.

1.4 The Contractor shall provide the services free of damaging software. This also applies to any software provided to the Principal (e.g., access software*). The Contractor furthermore warrants that the services are free of functions that endanger the integrity, confidentiality and availability of the Principal's data or other data provided by the Principal or software provided by the Principal and that run counter to the confidentiality or security interests of the Principal through

- functions for undesired dumping/redirecting of data,
- functions for undesired modification/manipulation of data or the flow logic or
- functions for undesired import of data or undesired function alterations.

A possible activity of a function is undesirable if the activity is neither requested by the Principal in its service description, nor offered by the Contractor with a specific description of the activity and its mode of operation, nor meets the requirements of the C5 requirements catalogue according to section 1.2.

1.5 Any inclusion of Contractor-side GTC* on the type and scope of the Cloud Services, which have been included as an Annex to the Contract, shall be subordinate to the Contract and to the EVB-IT Cloud

GTC, and only to the extent that they neither conflict with nor restrict all other contractual provisions. The Contractor's GTC* on the type and scope of the Cloud Services are also effectively included as above if they provide for a dynamic reservation of the right to make changes, insofar as the changes are not to the detriment of the Principal and have been made known to the Principal. Notwithstanding the foregoing, with regard to individual specific requirements, corresponding provisions from the Contractor's GTC* on the type and scope of the Cloud Services shall take precedence over the EVB-IT Cloud GTC, if this is expressly agreed in the criteria catalogue.

2 Nature and scope of the services

2.1 Software and Platform as a Service (SaaS* and PaaS*)

2.1.1 Insofar as a SaaS* or PaaS* service is owed, the Contractor shall provide the Principal with the application/platform agreed in the contract for use in a cloud infrastructure operated by the Contractor, including the necessary accesses, from the agreed provision time. The Contractor shall ensure the agreed availability in accordance with clause 8.1, the agreed quality of the service (functional and non-functional) as well as security within the scope of its responsibility during the entire term of the service. In particular, the Contractor shall dimension the cloud infrastructure and the application or platform in such a way that it is available with an appropriate response and execution speed with regard to the expected or agreed accesses and with a current security patch sufficient for the intended use or available for the agreed storage space and also otherwise in accordance with the agreed requirements. Insofar as the Principal operates applications on the platform in the case of PaaS*, it shall be responsible for these, their availability, content, and architecture as well as their performance as well as for its development activities. The Principal shall not perform or authorise any penetration tests in the respective cloud infrastructure without the Contractor's prior consent.

Furthermore, the scope of the services is set down in the contract.

2.1.2 Insofar as agreed, the Contractor shall be obliged to install and integrate the programme versions* of the application/platform agreed in the contract. This shall be done in each case within a reasonable period after the programme version* is available, but in compliance with section 2.1.5.

2.1.3 Insofar as agreed in the case of SaaS*, the Contractor shall be obliged to install and integrate program statuses* to implement changes to such legal provisions and technical standards which affect the usability of the application/platform for the intended use. In addition, further cases may be agreed in the contract in which programme versions* are to be installed and integrated. This may include, for example, adaptations to amended administrative regulations, tariffs, or interface adaptations. If such programme versions* are not available, the Contractor shall create them or have them created.

2.1.4 Insofar as an obligation exists in accordance with section 2.1.2 and/or 2.1.3, the Contractor shall install and integrate the due programme statuses* within a reasonable period of time prior to, but no later than, the entry into force of the respective regulation or standard or the date of the intended amendment or adaptation. If this is not done by these dates at the latest, the Contractor shall be obliged, without prejudice thereto, to provide the Principal with an interim solution. If the Contractor cannot reasonably be expected to do both by these dates, the service must be provided within a reasonable period of time.

2.1.5 The Contractor is obliged to inform the Principal in good time (e.g., by email or via the administration console) of the intention to make system adjustments in order to avoid incompatibilities, interruptions, and other disruptions.

2.2 Infrastructure as a Service (IaaS*)

- 2.2.1 Insofar as an IaaS* service is due, the Contractor shall make the cloud infrastructure agreed in the contract available to the Principal for use from the agreed time of provision and shall ensure the agreed availability, the agreed quality of the service (functional and non-functional) as well as the security of the cloud infrastructure. section 2.1.1 sentences 3 et seq. apply accordingly.
- 2.2.2 The Principal is responsible for compliance with the agreed access and system requirements. In addition, the Principal is responsible for operating systems, software, applications, and content not originating from or provided by the Contractor which it operates on this cloud infrastructure.
- 2.2.3 The Contractor shall provide the Principal with access to the agreed cloud infrastructure for its own use. The Principal is entitled to process data and operate programs on the cloud infrastructure. The Principal shall not perform or authorise any penetration tests in the respective cloud infrastructure without the prior consent of the Contractor.

2.3 Managed Cloud Services (MCS*)

- 2.3.1 Insofar as an MCS* service is due, the Contractor shall take over services to the agreed extent in connection with SaaS*, PaaS* or IaaS*, for which the Principal is otherwise responsible (e.g., cooperation services in accordance with section 17) as well as further services (e.g., consulting services or work to establish access).
- 2.3.2 Insofar as in addition to SaaS*, PaaS* or IaaS* services agreed with the Contractor MCS* services are due for these services, the Contractor shall provide these in addition to the SaaS*, PaaS* or IaaS* services.
- 2.3.3 Insofar as SaaS*, PaaS* or IaaS* services are not due by the Contractor, the Contractor shall not be responsible for these third-party services, even if the integration, control or use of the third-party services is part of its services.

3 Prohibitions of use

- 3.1 Neither the Principal nor the users who access the Contractor's services via the Principal are entitled to use the services,
- in a manner which is prohibited to the Principal by law, statutory instrument or official order known to the Principal,
 - to violate the rights of others.
- 3.2 Unless the intended use of the service is explicitly described, the use of the service in high-risk areas is excluded (operation of nuclear power plants, air traffic control systems, weapons of war, life-support equipment or comparable high-risk applications in which service failures typically lead directly to the death of people or to major emergencies).
- 3.3 Infringements of the prohibitions of use pursuant to section 3 shall entitle the Contractor to suspend its service, provided that it has set the Principal, or at least the person designated pursuant to section 6.2.2, a reasonable period of time to end the infringements before suspending the service and this period has expired unsuccessfully. If the Principal ends the infringement, the performance shall be resumed without delay. Insofar as the services affected by the suspension are suspended for more than 10 hours in the reference period*, the Principal shall also not owe any remuneration for the suspended service.

4 Place of performance

The storage and other processing of the Principal's data by the Contractor shall take place exclusively within the EU and the EEA as well as, if an adequacy decision pursuant to Art. 45 GDPR exists, Switzerland, unless the Principal has additionally selected other regions for the services in the administration console (self-service portal or similar). The processing of metadata within the meaning of requirements catalogue C 5 (in version 2020: OPS 11) is possible irrespective of sentence 1 in accordance with its provisions, insofar as the measures required therein for the secure handling of the metadata are actually implemented; for personal metadata, the regulations on the processing of personal data apply with priority.

5 Access / Storage space

- 5.1 The service shall be accessed via the public Internet using a market-standard web browser without inappropriate or non-market browser settings and without special access software. The transfer point is the Contractor's gateway to the Internet.
- 5.2 If access to the performance with special access software has been agreed, the Contractor shall be obliged to make this available to the Principal in good time.
- 5.3 The Contractor is obliged to prevent access to the Principal's data by unauthorised bodies and persons by taking appropriate measures.
- 5.4 Access by the Contractor or third parties to the Principal's data shall only be permitted in the agreed cases and shall be limited to the extent necessary for these cases. At the request of the Principal, the Contractor shall present the measures it has taken for this purpose within a reasonable period of time.
- 5.5 If the Principal cannot determine the size of the storage space available to it, e.g., by configuring the service, and if no specific size has been agreed, the Contractor shall provide the Principal with sufficient storage space for the contractual use of the service.

6 Data protection, IT security and confidentiality

The following provisions are without prejudice to further legal and regulatory requirements.

6.1 Data protection

- 6.1.1 The Parties shall comply with the provisions on data protection applicable to them in each case during provision of the service, as amended from time to time. The Contractor shall have sufficient documentation on the implementation of the statutory requirements, which the Contractor shall make available to the Principal upon request.
- 6.1.2 The Contractor shall ensure that all persons entrusted by it with the processing of personal data of the Principal comply with the provisions on data protection applicable to the Contractor. Insofar as a commitment to data secrecy is required, this shall be made at the latest before the first commencement of the activity and submitted to the Principal upon request.
- 6.1.3 If the subject of the commissioned service is at least also the processing of personal data, the Parties shall conclude a contract processing agreement (CPA) prior to the processing of personal data by the Contractor on behalf of the Principal. In the course of concluding the CPA, the Parties shall take appropriate technical and organisational measures (TOM). In each case, the minimum requirements for the service from these EVB-IT Cloud GTC, the EVB-IT Cloud Contract as well as the requirements pursuant to

Articles 28 and 32 of the GDPR and other legal provisions applicable to the Contractor as a processor must be fully complied with.

- 6.1.4 To the extent required by law, the Contractor shall appoint a company data protection officer with the necessary expertise and shall provide the Principal with their contact details upon request.

6.2 IT security

- 6.2.1 The Contractor shall have an appropriate, documented and implemented security concept and an information security management system (ISMS) for the provision of the service (including the necessary infrastructural, organisational, personnel and technical components), in each case in accordance with ISO 27001, including emergency management. The security concept shall be aligned with ISO 27017. If personal data is processed, it must also be aligned with ISO 27018.

Insofar as agreed, the Contractor shall prove this by means of valid certificates or equivalent evidence. The security concept, ISMS and certificates must, insofar as they are applicable to the service to be provided, fully cover the service, and must be renewed in accordance with the specified audit frequency in the relevant standard.

- 6.2.2 The Contractor shall have an IT security officer with the necessary expertise and shall provide the Principal with their contact details upon request. The Contractor shall inform the Principal promptly and in an appropriate form of security incidents* affecting it. If the Principal has appointed an IT security officer or another person to receive such information, the information shall be sent directly to this person.

6.3 Confidentiality

- 6.3.1 The Parties are obliged to treat all confidential information, business and trade secrets obtained within the framework of the contractual relationship as confidential, in particular not to pass them on to unauthorised third parties or to use them other than for contractual purposes. The aforementioned duty of confidentiality shall not, however, restrict any party from using in other projects persons working for it who have had access to confidential information. The exchange of experience of the Principal with and within the public sector remains unaffected, as does the fulfilment of legal obligations.

- 6.3.2 Confidential information is information which a reasonable third party would consider worthy of protection, or which is marked as confidential; this may also be information which becomes known during an oral presentation or discussion. Confidential information may only be used or exploited for the purpose of fulfilling the obligations under the contract. The obligation of confidentiality does not apply to information that is already lawfully known to the parties or becomes known outside the contract without a breach of a confidentiality obligation.

6.4 Audit rights

- 6.4.1 The Contractor is obliged to provide evidence of compliance with the IT security requirements. At the request of the Principal, the Contractor shall in particular provide the security evidence required in accordance with the Minimum Standard for External Cloud Services of the BSI; this may also be provided by the regular provision of a current C5 Type2 report. At the request of the Principal, the Contractor shall also provide evidence of the regular performance of audits, security checks, penetration tests and vulnerability analyses, e.g., through corresponding confirmations by auditors.

6.4.2 If the Principal has doubts with regard to the documents provided by the Contractor pursuant to section 6.4.1, which the Contractor is not able to clarify upon request within a reasonable period of time, the Contractor shall be obliged to grant access to appropriately qualified or trained personnel of the Principal, or an independent auditing company commissioned by the Customer during normal business hours. The Contractor is obliged to grant appropriately qualified or trained personnel of the Principal or of an independent auditing company commissioned by the Principal and bound to professional secrecy access during normal business hours in particular to the processing systems, facilities and supporting documents relevant to the processing of the Principal's data, so that the Principal can verify whether the Contractor is complying with the requirements. The audit shall be carried out with due regard for the security concerns and the business and trade secrets of the Contractor and the Contractor's other customers. The Contractor shall be responsible for ensuring that the inspection can nevertheless be carried out effectively and to the required extent. Each party shall bear its own costs for such audits. Where appropriate, the audit should be based on the ISACA Germany Chapter e.V. guide "Application of BSI C5 by Internal Audit and Information Security". The principles of proportionality and economic efficiency are to be maintained in the interest of all parties. If the result of the audit only reveals insignificant objections, the Principal shall pay a fee if such a fee is provided for in the catalogue of criteria.

6.4.3 The audit shall be carried out with reasonable advance notice to the Contractor and in compliance with the contractual confidentiality rules. In principle, it shall take place only once within a 12-month period, unless there is a special reason for doing so. Before the start of such an audit, the Principal shall inform the Contractor of the initial subject of the audit and the planned scope so that the Contractor can plan accordingly. The Parties shall agree on the place, date, and contact person.

6.5 Legal consequences of non-compliance

The Principal may terminate the contract in whole or in part within a reasonable period of time if the Contractor with regard to its obligations under sections 6.1 to 6.4:

- culpably fails to comply within a reasonable period set or
- violates these duties intentionally or with gross negligence.

There is no right of termination if the breach of duty is immaterial.

Insofar as the aforementioned breaches of duty concern services to be provided on a one-off basis, the right of termination shall be replaced by the right to withdraw from the respective service.

7 Data security service/backup/return and deletion entitlement

7.1 The Contractor shall be obliged to delete data securely and in accordance with the standards applicable at the time of deletion within a reasonable period of time at the request of the Principal or to grant the Principal a corresponding deletion option. In the case of personal data, the provisions of the CPA shall also apply. This shall not apply insofar as the Contractor is obliged to retain certain data under the law of the EU or a Member State. In the event of such a storage obligation, the Contractor is obliged to inform the Principal immediately, to protect the data securely from access by third parties and, insofar as permissible within the scope of the statutory storage obligation, to store it in encrypted form in accordance with the current state of the art.

7.2 Insofar as the creation of backups of the Principal's data has been agreed, the Contractor shall be obliged, at the Principal's request, to restore data from a backup to the existing status requested by the Principal within a reasonable period of time.

- 7.3 The service shall be designed in such a way that the Principal's data can either be exported independently at any time by the Principal or, if this is not possible for technical reasons, with the Contractor's support from the cloud infrastructure in a market-standard exchange format. This means that it must also be possible to export parts of the data specified by the Principal. Insofar as the data are encrypted, this obligation is only fulfilled if the Principal has the key. The Principal is responsible for exporting the data and for securing it during the export.

8 Availability

- 8.1 The Contractor shall owe the agreed availability of the service at the due transfer point using the agreed access during the operating hours*. The connection of the Contractor's data centre to the transfer point shall be sufficiently dimensioned so that the use of the service is not restricted even under a contractually agreed maximum load (e.g., an agreed quantity structure or another agreed dimensioning).

The percentage of availability is calculated according to the following formula:

$$\text{Availability} = \frac{\text{Total time in minutes} - \text{downtime in minutes}}{\text{Total time in minutes}} * 100$$

The total time in minutes results from the agreed operating time* per calendar month. Downtime* is those minutes during which the Principal is unable to establish connectivity to the cloud infrastructure to be provided by the Contractor within the operating hours* or the affected service is not available as a whole or not available in all its essential basic functionalities for more than an insignificant part of the users.

- 8.2 Periods of planned unavailability shall not reduce the availability unless they fall within an agreed core operating time*.
- 8.3 The following applies with regard to availability:
- The Contractor shall owe an availability of at least availability class* VK1 in the reference period during the operating time*.
 - The reference period is the calendar month.
 - All times are given according to Central European Time (CET) or Summer Time (CEST).
 - The operating time* is the time from Monday to Sunday from 0:00 to 24:00.
 - The time from 04:00 to 08:00 on Sundays is time of planned unavailability (e.g., for maintenance work) and is not taken into account in the calculation of availability.
 - Downtime* due to any of the following events will not reduce availability:
 - o Problems within the network or infrastructure of the Principal or of third parties commissioned by the Principal,
 - o Failure/impairment of the Principal's network connection,
 - o Failures/impairments due to the actions or omissions of the Principal or a third party not commissioned by the Contractor,
 - o non-contractual use by the Principal of the Contractor's service,

- o Failure of the Principal to comply with agreed specifications on required configurations and architectures as well as incorrect entries or instructions by users of the Principal,
 - o Actions of unauthorised users, insofar as the possibility of action of the unauthorised user is attributable to the Principal (e.g., through the non-observance of appropriate security procedures),
 - o Suspension of access due to a security incident* for the protection of the Principal as well, provided that the internal guidelines (operational measures), which are the basis for the fulfilment of the C5 requirements, are comparable to the IT basic protection modules DER.2.X "Security Incident Management" of the BSI and allow a suspension as a measure due to the severity of the security incident*,
 - o events that are due to force majeure and cannot be compensated for by reasonable measures taken by the Contractor.
- The Contractor is responsible for measuring availability.

9 Reporting obligations

9.1 With regard to the Contractor's reporting obligations, the following is agreed:

- The Contractor shall be responsible for ongoing monthly reporting to the Principal; reporting shall include at least the following information with regard to availability and any agreed response and recovery times:
 - o recording the times of availability and unavailability,
 - o the resulting availability/unavailability per reference period and
 - o safety-relevant disruptions* which occurred during the reference period, and which affect the service and, if applicable, have already been rectified,
 - o disruptions reported by the Principal in the reference period and their processing status (if applicable, via a ticket system used)
 - o recording the overrun (in minutes) of agreed response or recovery times per overrun case.
 - o In the case of use-based remuneration, the reporting includes all parameters relevant to remuneration.
 - o Reporting also includes any credits owed, although these can alternatively be shown in the statement.

9.2 The reporting shall be provided or made available immediately after the end of the respective reporting period in electronic form, e.g., for download on an access-protected website (e.g., an administration console), and explained to the Principal at its request.

9.3 The Principal has rights to the reports in accordance with section 14.1, whereby the rights of use are not limited in time.

9.4 In the event that the Contractor does not fulfil its reporting obligations even after the expiry of a reasonable deadline set by the Principal, the Principal shall be entitled to an appropriate credit.

10 Disruption classification

A distinction is made between the following three classes of disruption:

- 10.1 A serious disruption* shall be deemed to exist if the use of the affected service is impossible or severely restricted, either in whole or in specific functions, for more than an insignificant proportion of the Users authorised by the Principal in accordance with the contract.
- 10.2 A significant disruption* shall be deemed to exist if the use of the affected service is significantly restricted. A significant disruption* shall also be deemed to exist if the slight disruptions* as a whole lead to a not insignificant restriction of the use of the affected service.
- 10.3 A minor disruption* is deemed to exist if the use of the affected service is possible without or with insignificant restrictions.

11 Troubleshooting

- 11.1 If a disruption* occurs in SaaS* or PaaS*, the Contractor shall take all measures necessary to eliminate the disruption and restore operational readiness*. These may include, for example, repair services or maintenance services for the software used to eliminate disruptions*. If the disruption lies in third-party software used, the Contractor shall be obliged to use a programme version* that eliminates the disruption*, provided such a version is available. If this is not the case, the Contractor shall provide a workaround solution*. If this is unacceptable to it, it shall make every effort to obtain from the manufacturer of the third-party software the earliest possible provision of a program version* that eliminates the disruption*. At the Principal's request, the Contractor shall provide information on this. If no reaction times* have been agreed, the rectification of the disruption shall be started immediately after receipt of the corresponding notification or occurrence of the agreed event within the agreed service times*. If no recovery times* have been agreed, the rectification of the disruption* shall be completed within a reasonable period. If the Contractor does not comply with agreed response and/or completion times*, it shall be in default after exceeding them even without a reminder, unless it is not responsible for exceeding the deadline.
- 11.2 If a disruption occurs in IaaS*, the Contractor shall take all measures necessary to eliminate the disruption and restore operational readiness*. If no reaction times* have been agreed, the disruption rectification shall be started immediately after receipt of the corresponding message or occurrence of the agreed event within the agreed service times*. If no completion times* have been agreed, the disruption rectification shall be completed within a reasonable period of time. If the Contractor fails to comply with agreed response and/or completion times*, it shall be in default after exceeding them even without a reminder, unless it is not responsible for exceeding the deadline.

12 Modification of the service after conclusion of the contract by the Contractor

In order to improve the functionality of the services or to adapt the services to the state of the art, the Contractor may adapt the services after the commencement of the contract without the Principal's consent. However, such a change must not result in the originally agreed functionalities no longer being available to the Principal or in originally agreed requirements only being met to a significantly limited extent. Changes or restrictions are in any case substantial and thus inadmissible if they would have led to a worse evaluation of the services in the award procedure.

13 Duties and performances in connection with the end of the contract

13.1 Provision of information, availability

Pursuant to section 7.3, the Contractor is obliged to make the Principal's data available (e.g., by offering the possibility of downloading) without separate remuneration. The Principal is at liberty to request that the data be made available in a format other than the agreed format unless this is unreasonable for the

Contractor. Insofar as this form of provision demonstrably leads to a significant additional expense, the Contractor may make the provision dependent on the agreement of a separate remuneration to be agreed.

13.2 Migration support

The Principal shall be responsible for the migration to another system. Insofar as agreed, the Contractor shall be obliged, upon request and to a reasonable extent, to provide services which are necessary to enable a new Contractor or the Principal to take over the service. In this context, the Contractor owes the following services in particular:

- 13.2.1 Within the scope of an agreed migration pursuant to section 13.2, the Contractor shall, at the request of the Principal, consult with the contact person of the planned successor for the provision of services, provided that this contact person has been demonstrably committed to confidentiality vis-à-vis third parties in advance. The Contractor shall coordinate with the successor the necessary services, in particular those required in connection with the transfer, e.g., a migration concept. Irrespective of this, the Contractor is obliged to cooperate appropriately with the planned successor and to ensure, as far as possible, that no serious or significant disruptions to the provision of the service owed occur during the transfer. The successor shall be obliged accordingly. Remuneration for migration support shall be based on time and material at the agreed remuneration rates.
- 13.2.2 Insofar as the migration is delayed, irrespective of the reason, the Contractor shall continue provision of the service once at the request of the Principal to the previous extent beyond the original end of the contract until the transfer has been successfully completed, irrespective of this, however, for a maximum period of six months. The service shall be provided at the previous conditions. In the event that the Contractor incurs additional expenses due to necessary services, the Contractor may demand an appropriate adjustment of the remuneration.

13.3 Duties in accordance with availability and migration

- 13.3.1 Insofar as changes or additions have been made to the items mentioned therein and/or to the stored data after they have been made available in accordance with section 13.1, these shall be made available again at the Principal's request, insofar as they have not been lawfully deleted.
- 13.3.2 The Contractor shall enable the Principal to securely, i.e., non-reconstructibly, delete or mark for deletion the data stored by it at a time determined by the Principal, in which case the Contractor shall securely, i.e., non-reconstructibly, delete the data. The deletion shall be proven to the Principal upon request and by means of a corresponding declaration or otherwise. The deletion procedure shall be proven upon request. The Contractor's statutory obligations to retain data shall remain unaffected, taking into account the provisions in section 13.1.
- 13.3.3 The Principal shall remain entitled to export the data pursuant to section 7.3 until it is deleted. The Contractor shall be obliged to provide the interface required for this purpose; this shall apply for a period of three months after the end of the contract, insofar as deletion has not yet taken place by this time. If these services involve more than insignificant effort on the part of the Contractor after the end of the contract, the Contractor shall be entitled to reasonable, but in no case higher, remuneration.

14 Rights of use

- 14.1 Upon provision, the Contractor shall grant the Principal the non-exclusive, non-transferable right, limited in time to the term of the contract, terminable or suspendable in accordance with the contractual agreement on an ordinary basis and otherwise only on an extraordinary basis, to use the service including any access software* physically provided for the use of the performance, taking into account any quantitative metrics provided for in the contract such as number of users, volume, etc., i.e. also to temporarily store and load the software provided and to display and run it to the extent necessary for the intended use of the service. This also means temporarily storing and loading the software provided, displaying it, and running it, insofar as this is necessary for the intended use of the service. This shall also apply insofar as duplications are necessary for this purpose. The right of use shall exist worldwide except for those countries in which the Contractor does not generally offer the respective service due to governmental legal acts (e.g., export restrictions) and access to the service is not possible as intended. Access is not possible for the intended purpose if, in the case of an applicable geolocation, access is blocked for all customers in the country concerned due to governmental legal acts. Upon request, the Contractor shall immediately inform the Principal of the countries in which the Contractor does not make the services available due to the aforementioned regulation. The aforementioned rights shall apply without prejudice to further rights to services to be provided individually pursuant to section 14.2.
- 14.2 Insofar as individual services are agreed, the Contractor shall grant the Principal the non-exclusive, spatially unrestricted, transferable, permanent, irrevocable and non-terminable right, exercisable in any hardware and software environment, to use, modify, translate, edit or otherwise transform the individual services in the original or in modified, translated, edited or redesigned form on any known medium or in any other way, to reproduce, exhibit, distribute in tangible or intangible form, to publish with the exception of any source code provided, to have third parties use it for its intended purpose, to have it operated for the Principal, to use it not only for its own purposes but also for the provision of commercial and non-commercial services to Principals pursuant to sections 99 to 101 GWB as well as non-commercial services to other third parties.
- 14.3 If and to the extent that data, databases or database works or other results (e.g. software, documents) are created by the Principal's use of the services, the Principal shall be entitled to all rights under section 14.2 to the works newly generated by it with the proviso that it shall hold these rights exclusively and that the restrictions on the rights of the Principal agreed therein, in particular to publication as well as to use, shall not apply to services provided to third parties. Insofar as the works newly generated by the Principal include services of the Contractor (e.g., libraries) as an integral part or the exercise of the rights to the works requires the use of services of the Contractor, the respective rights pursuant to section 14.1 or section 14.2 shall remain in force with regard to the use of such services of the Contractor. The Principal grants the Contractor rights to the works newly generated by the Principal with which it uses the service or which it incorporates into the service, limited to a maximum of the term of the contract, to use these works exclusively for the performance of the contract and to the extent necessary for this purpose.
- 14.4 Insofar as the use of services by the Principal after the end of the contract has been agreed, the Principal shall be entitled to the rights of use required for this purpose.
- 14.5 The Principal grants the Contractor and the third parties involved in the performance of the services the rights to the data and software brought in by the Principal that are necessary for the performance of the services.

15 Subcontractor

- 15.1 The Contractor may only use subcontractors for the performance of the services or replace subcontractors used if the Contractor names the subcontractor(s) and their respective scope of performance (type and scope of outsourcing to the subcontractor). The designation can be omitted if it is only a matter of subcontractors or such companies whose performance does not concern any agreed C5 criteria, and which are not involved in the provision of the services or only provide ancillary services.
- 15.2 Insofar as agreements are to be changed in the relationship between the Contractor and the subcontractor which affect the agreed C5 criteria, the Contractor shall notify the Principal thereof. The designation or notification of planned contractual changes can also be made by means of a website accessible to the Principal in connection with an individual notification, e.g., by push message. The Principal is entitled to object to the use of subcontractors or the aforementioned changes for objective reasons within 30 days of the individual notification. If the Parties cannot agree on the planned contract amendment or the replacement of the subcontractor within 90 calendar days of receipt of the individual notification, the Principal has the right to terminate the contractual relationship in whole or in part without notice.
- 15.3 Insofar as agreed, it shall apply alternatively to section 15.1 that the Contractor may only use subcontractors for the performance of services or may only replace subcontractors used if the Contractor names the subcontractor(s) and the Principal expressly consents to their use. A prerequisite for consent is first of all that the subcontractor, insofar as this relates to its services, has previously undertaken vis-à-vis the Contractor to comply with the contractual provisions to at least the same extent as the Contractor undertakes to comply with the contractual provisions vis-à-vis the Principal and the Contractor proves this to the Principal upon request. Consent is also required if the Contractor itself now intends to provide a service which it has previously provided via a subcontractor. The Principal shall give its consent if, taking into account the new subcontractor or the Contractor instead of the old subcontractor, no other decision for award of the contract would have resulted and there is also no other objective reason to oppose the use of the subcontractor. The new subcontractor shall be trained at the Contractor's expense. The consent of the Principal shall be deemed to have been given for the subcontractors named in the tender of the Contractor or otherwise in the award procedure.
- 15.4 A prerequisite for the use of a subcontractor is that the subcontractor, insofar as this concerns its services, has previously undertaken to comply with the contractual provisions vis-à-vis the Contractor to an extent corresponding to its respective share in the provision of the services, as the Contractor has done vis-à-vis the Principal.
- 15.5 The Contractor may only pass on confidential information to subcontractors whose use the Principal has not expressly objected to and only if and insofar as this confidential information is necessary for the provision of the respective services by the subcontractor ("need-to-know" principle) and the subcontractor is obliged to confidentiality to at least the same extent as the Contractor.
- 15.6 Subcontractors in this sense are also those who are in turn used by subcontractors (subcontractor chain).

16 Remuneration

- 16.1 The remuneration for the services can be made in the form of monthly lump sums, according to use through use-dependent remuneration ("pay-as-you-go") or effort-related remuneration (for example according to time spent). The remuneration is due on the 15th of the month following the provision of the service.
- 16.2 If remuneration for a service provided by Contractor personnel has been agreed on the basis of time spent, the following shall apply:
- 16.2.1 In the case of remuneration according to time spent for services pursuant to section 16.2, all other costs, in particular ancillary costs, travel expenses and material costs, shall be compensated with the remuneration for time spent. Travel time shall not be remunerated. The remuneration shall be due on the 15th day of the month following the performance of the service.
- 16.2.2 If an upper limit has been agreed in the case of remuneration according to time spent pursuant to section 16.2, the Contractor shall be obliged to provide the agreed service in full even if this limit is exceeded. This shall not apply if the Contractor is not responsible for the overrun. In this case, however, the Contractor shall be obliged to provide the agreed service in full for additional remuneration according to time and material at the agreed rates if the Principal so requests.
- 16.2.3 No more than one daily rate shall be paid per calendar day in the case of remuneration on a time and material basis in accordance with clause 16.2. An agreed daily rate can only be invoiced if at least eight hours have been worked. If less than eight hours are worked per day, these shall be invoiced on a pro rata basis. If an hourly rate has been agreed, hours started shall be remunerated on a pro rata basis. Breaks shall be indicated and shall not be remunerated. If more than six hours are worked, it shall be assumed that the Contractor has taken a half-hour break. This shall not apply if the Contractor proves that they did not take a break.
- 16.3 Any remuneration due shall be paid within 30 days of receipt of an auditable invoice. Invoices shall be issued and transmitted in electronic form in accordance with the E-Invoice Regulation. In the case of recurring remuneration, a single auditable standing invoice shall be sufficient as long as the remuneration has not changed.
- 16.4 Credits owed shall be deducted from the remuneration in the invoice. Otherwise, the Principal may itself offset these against remuneration owed or demand payment of the credits owed, insofar as offsetting is not possible.
- 16.5 If a price adjustment for services has been agreed, the following shall apply unless otherwise stipulated: An increase in the remuneration may be announced for the first time 12 months after the commencement of the provision of the services, and further increases at the earliest 12 months after the previous increase takes effect. An increase shall become effective three months after the announcement. The increase must be reasonable and in line with the market and may not exceed 3% of the remuneration applicable at the time of the announcement of the increase.
- 16.6 All prices are net and, insofar as VAT is payable, plus the applicable statutory VAT.

17 Cooperation of the Principal

- 17.1 The Principal shall be responsible for the cooperation performances listed in the contract. It shall provide the Contractor with the necessary information and documents from its sphere.
- 17.2 The Principal shall maintain appropriate security standards for the use of the services by its users. The Principal shall be responsible for complying with the "Corresponding Criteria for Principals" from the respective

status of the requirements catalogue C5 of the BSI agreed for the contractual service in accordance with section 1.2.

- 17.3 The Principal shall be responsible for ensuring that the systems and data which it makes accessible to the Contractor in the course of the provision of services may also be operated or processed by the Contractor for this purpose.

Within the scope of commissioned processing, the Principal shall check on its own responsibility whether the data transmitted by it to the Contractor in connection with the use of the service constitute personal data and whether the processing of these personal data is permissible by way of contract processing.

- 17.4 The Principal is responsible for the type and content of the data and software made available to the Contractor.
- 17.5 If the Principal uses the services - e.g., IaaS* - in order to make software and other service offerings available to the users, it shall also be responsible for their use. The Principal shall inform the respective users to the required extent about the services relevant to them, their limits and about relevant cooperation services.
- 17.6 The Principal shall report disruptions* or defects, providing the information known to it and useful for their detection. A report in the administration console or an entry in a ticket system shall be sufficient. If the report is made informally, the Contractor shall immediately enter the disruption report in the system provided for this purpose (administration console or ticket system).
- 17.7 In the case of an agreed remote service*, the Principal shall provide the necessary technical equipment at the Principal's premises in accordance with the contractual agreements, insofar as this is necessary for access to the system.
- 17.8 The Principal shall also be responsible for using the functionalities in an administration console provided by the Contractor, in particular for naming the authorised recipients for messages from the Contractor.
- 17.9 The Principal shall take commercially reasonable measures to prevent or terminate any unauthorised access or use via the accesses provided to it.
- The Contractor's obligation to take reasonable measures to protect the service and access thereto from unauthorised access is unaffected. The Principal shall not be liable for unauthorised access if such access could have been prevented by such measures taken by the Contractor.
- 17.10 Upon a corresponding notice by the Contractor that additional commissioning of services not covered by the award procedure, or the contract is possible via access to the services, e.g., with the help of an administration console, the Principal shall in this respect take appropriate organisational measures to monitor the type and scope of the use of the services.

Insofar as the Contractor provides the Principal with corresponding administration options, in particular a rights and roles structure, the Principal shall be responsible to the extent made possible by this for preventing the possible commissioning of additional services by the Contractor via the administration console.

18 Rights of the Principal in the Event of Defects in the Services

The Contractor shall provide the Principal with the agreed service during the term of the contract in accordance with the contract. For the period in which the usability of the service is not possible due to

a defect or poor performance, the Principal shall only pay an appropriately reduced remuneration for the performance, insofar as no other compensation (such as non-performance credits) has been agreed for this poor performance.

The Principal's other statutory claims due to defects or poor performance shall remain unaffected.

19 Limitation of liability

In the absence of any other contractual liability agreement, the following provisions shall apply to all statutory and contractual claims for damages, indemnification, and reimbursement of expenses of the Principal:

- 19.1 In the event of slightly negligent breaches of duty, liability for the contract as a whole shall in principle be limited to the contract value*. In this case, however, the liability shall amount to at least twice and at most four times the remuneration payable for the first year of the contract. If the contract value* is less than 50,000 euros, liability shall be limited to 50,000 euros. In the event of damage to property, liability shall be limited to one million euros if the contract value* is less than one million euros.
- 19.2 Unless otherwise agreed, claims for loss of profit are excluded.
- 19.3 The limitations of liability shall not apply to claims based on intent and gross negligence, in the event of injury to life, limb or health, in the event of fraudulent intent, insofar as the Product Liability Act applies and in the event of warranty promises.

20 Term and termination

- 20.1 If no end of the respective contract term has been agreed, it may be terminated in whole or in part with six months' notice to the end of a calendar month, but no earlier than the end of an agreed minimum contract term. A different period of notice may be agreed in the contract.
- 20.2 In addition, the contract may be terminated in whole or in part by either Party for good cause - without observing a notice period - within a reasonable period of time after knowledge of the reason for termination. Good cause shall be deemed to exist if facts are given on the basis of which the terminating Party, taking into account all circumstances of the individual case and weighing the interests of the contracting Parties, can no longer be expected to continue the contract. If the good cause consists in the breach of a contractual obligation, the termination is only permissible after the unsuccessful expiry of a deadline set for remedial action or after an unsuccessful warning, unless a notice of termination is given in accordance with section 314 in conjunction with section 323 (2) of the German Civil Code (BGB). In the event of termination for good cause, the Contractor shall be entitled to remuneration for the services rendered under the contract up to the effective date of the termination. However, the remuneration shall not be paid for such services for which the Principal demonstrates that they are of no interest to it due to the termination.

21 Liability insurance

- 21.1 Insofar as agreed, the Contractor shall prove to the Principal upon conclusion of the contract that it has industrial liability insurance or comparable insurance from a member state of the EU that is customary in the market in terms of scope and extent.
- 21.2 The Contractor shall maintain this insurance cover until the end of the contract and beyond that until all claims for defects become time-barred. If the Contractor fails to comply with this the Principal shall be

entitled to terminate the contract after setting a reasonable deadline if it can no longer reasonably be expected to adhere to the contract. Further claims of the Principal, in particular claims for damages, shall remain unaffected by this.

22 Rights of retention and rights to refuse performance

The Contractor's rights of retention and rights to refuse performance shall be excluded without prejudice to clause 3, unless the Principal does not dispute the underlying counterclaims, or these have been legally established. This shall also apply to any lessor's lien in respect of hosted data and applications of the Principal.

23 Text form

Unless otherwise stipulated, contractual notices and declarations must at least be in text form. Entries in the administration console* shall also be in text form. An entry in a ticket system is sufficient for disruption reports and notices of defects.

24 Applicable law, place of jurisdiction

- 24.1 The law of the Federal Republic of Germany shall apply to the exclusion of the norms referring to another legal system and to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG).
- 24.2 If the conditions exist for an agreement on the place of jurisdiction according to section 38, 40 of the German Code of Civil Procedure (ZPO), the place of jurisdiction for all disputes concerning the validity of the contract and arising from the contractual relationship shall be exclusively determined by the registered office of the office responsible for representing the Principal in the proceedings. Upon request, the Principal shall be obliged to inform the court of the office representing it in the proceedings.

Definitions

Contractor's GTC	General Terms and Conditions of the Contractor, its subcontractors and suppliers.
Contract Value	The contract value is the sum of all remunerations to be paid.
Downtime	Periods of unplanned unavailability of the service within the operating time.
Operational readiness	The service works without interference.
Operating time	Times during which the Principal is entitled to provision of the service.
Concurrent User	Concurrent users of a service, e.g., a SaaS* or PaaS*.
Data backup	Data backup includes all technical and organisational measures to ensure the availability, integrity and consistency of the data and software stored on the cloud infrastructure and used for processing purposes*.
Infrastructure as a Service (IaaS)	With IaaS*, IT resources such as computing power, data storage or networks are offered as a service. A Principal uses these virtualised and highly standardised services and builds its own services on top of them for internal or external use. For example, a Principal can use computing power, RAM, and data storage and run an operating system with its applications on it.
Core operating time	Agreed times within the operating hours in which the Principal is entitled to provision of the service with an increased scope of services, e.g., with a higher availability or a particularly short recovery time. Times of the planned unavailability are outside the core operating hours.
Managed Cloud Services (MCS)	Managed cloud services are services that go beyond the typical performance obligations of the Contractor, e.g., the user administration, if applicable the management of different cloud offerings or options, capacity management, consulting for upgrade and licensing issues, etc. - in each case geared to the individual needs of the Principal.
Monitoring	Examples of monitoring are: • Availability monitoring. Monitoring of the availability of all devices / services for which an availability and / or performance is defined.

- Disruption* monitoring. Monitoring of detected incidents and other status events on servers and network devices, including availability, process status, file system capacity and success/failure of backups.
- Performance monitoring. Monitoring of important performance metrics with regard to system resources, (e.g., CPU, memory, and data storage) and the applications being run (e.g., process statistics, users, throughput) and databases (e.g., caching, performance, transaction success).
- Security monitoring. Active monitoring of the infrastructure and services for vulnerabilities resulting, for example, from misconfiguration or the outstanding installation of security-relevant updates.

Named User	Users named by the Principal.
Patch	Temporary elimination of a defect and/or disruption* in the software without intervention in the source code*.
Platform as a Service (PaaS)	A PaaS provider provides a complete infrastructure and offers the Principal standardised interfaces on the platform that are used by the Principal's services. For example, the platform can provide multi-Principal capability, scalability, access control, database access, etc. as a service. The Principal usually has no access to the underlying layers (operating system, hardware), but it can run its own applications on the platform, for the development of which the Contractor usually offers its own tools.
Programme status	Generic term for patch*, update*, upgrade* and new release/version*.
Response time	Period of time within which the Contractor has to start with the disruption or defect rectification work. The period begins with the occurrence of the disruption, but only runs during the agreed service times*. If the disruption occurs outside these times, the response time shall begin with the next service time*.
Release / Version	New development stage of a software which differs significantly from the previous release* or version* in the range of functions and/or data (e.g., change of version number from 4.5.7 to 5.0.0).
Service time	Times within which the Principal is entitled to have disruption or defect rectification work carried out.
Security incident	An attack on the cloud infrastructure and the Contractor's services that • endangers the confidentiality, availability, or integrity thereof to such an extent that significant damage may occur or • the same is actually impaired.
Software as a Service (SaaS)	Refers to the provision of software or functions of software in an infrastructure operated by the Contractor.
Disruption	Impairment of the suitability of the service for the contractually agreed use or, in the absence of such an agreement, for the assumed use or otherwise for normal use. This shall apply

irrespective of responsibility and irrespective of whether this deviation already existed at the beginning of the service.

Bypass solution

Temporary bridging of a defect and/or disruption*.

Update

Bundling of several defect corrections and/or disruption rectifications as well as minor functional improvements and/or adaptations of the software* in a single delivery (e.g., change of version number from 4.1.3 to 4.1.4).

Upgrade

Bundling of several defect corrections and/or disruption rectifications and more than minor functional improvements and/or adaptations of the software* in a single delivery (e.g., change of version number from 4.1.3. to 4.2.0).

Availability classes

Classification of availability according to HV Compendium of the BSI Volume G, Chapter 2 in the version current at the time of the conclusion of the contract.

Availability class	Description	Minimum availability	Non-availability	Downtime per month	Downtime* per year
VK 0	Standard IT system without requirements for the availability	~95%	~5%	1 day	Several days
VK 1	Standard Security according to IT basic protection for normal availability requirement	99.0%	1%	< 8 h	< 88 h
VK 2	Standard Security according to IT basic protection for increased availability requirement	99.9%	0.1%	< 44 min	< 9 h
VK 3	Highly available according to IT Basic protection for specific IT resources; BSI-Standard 100-3	99,99%	0,01%	< 5 min	< 53 min

VK 4	Highest availability	99,999%	0,001%	< 26 s	< 6 min
VK 5	Disaster tolerant	max. availability	0	0	0

Restoration period

The period of time within which the Contractor is to remedy the disruption or defect. The period begins with the occurrence of the disruption* but only runs during the agreed service times. If the disruption* occurs outside of these times, the recovery time begins with the next service time.

Access software

Software required for access to the cloud infrastructure operated by the Contractor in order to use the services, e.g., an agreed application or platform.