



# Data Processing Agreement according to Art. 28 General Data Protection Regulation

of

Gentlent GmbH  
Am Trippelsberg 92  
40589 Düsseldorf  
Germany

This Data Processing Agreement ("DPA") applies to the processing activities of personal data by Gentlent GmbH (also referred to as "we" or "Contractor"), which are provided to Controller (hereinafter referred to as "Client" or "You") in performance of the Main Contract.

## Preamble

The Contractor shall provide services to the Client in accordance with the Main Contract concluded between them on the Services of the IT Service Agreement (hereinafter: "Main Contract"). Part of the performance of the Main Contract is the processing of personal data within the meaning of the General Data Protection Regulation ("GDPR"). In order to comply with the requirements of the GDPR for such constellations, the Parties conclude the following Data Processing Agreement (also "DPA" or "Agreement"), which comes into effect upon signing or entry into force of the Main Contract.

## 1. Object of DPA

1. Within the scope of the cooperation of the Parties in accordance with the Main Contract, the Contractor shall have access to personal data of the Client (hereinafter "Client Data"). The Contractor shall process this Client Data on behalf of and in accordance with the instructions of the Client within the meaning of Art. 4 No. 8 and Art. 28 GDPR.
2. The Client Data shall be processed by the Contractor in the manner described in the Annexes and to the extent and for the purpose specified therein. The group of persons affected by the data processing is shown. The duration of the processing shall correspond to the term of the Main Contract.
3. Whether the Contractor's services are suitable for the processing of special categories of personal data pursuant to Article 9 (1) of the GDPR requires a risk assessment by the Client.
4. The Contractor is prohibited from processing Client Data in a manner deviating from the processing specified in the Annexes.
5. The processing of the Client Data shall generally take place in the territory of the Federal Republic of Germany, in a member state of the European Union or in another state Party to the Agreement on the European Economic Area. Should there be a relocation of the commissioned processing to a third country, this shall require the prior consent of the Client and shall only take place if the special requirements of Art. 44 to 49 GDPR are met. The Client already consents to the processing of personal data by the subcontractors named in the Annexes upon conclusion of this Order Processing Agreement.
6. The provisions of this DPA shall apply to all activities related to the Main Contract. The same shall apply to all activities in which the Contractor and its employees or persons commissioned by the Contractor come into contact with Client Data.



## 2. Client's power of instruction

1. The Contractor shall process the Client Data within the scope of the commission and on behalf of and in accordance with the instructions of the Client within the meaning of Art. 28 GDPR (commissioned processing). The Client shall have the sole right to issue instructions on the type, scope and method of the processing activities (hereinafter also referred to as "right to issue instructions"). If the Contractor is required by the law of the European Union or the Member States to which it is subject to carry out further processing, it shall notify the Client of these legal requirements prior to the processing.
2. Instructions shall generally be issued by the Client in writing or in electronic form (email is sufficient); instructions issued verbally shall be confirmed by the Contractor in electronic form.
3. If the Contractor is of the opinion that an instruction of the Client violates data protection provisions, it shall notify the Client thereof. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client.

## 3. Protective measures of the Contractor

1. The Contractor shall be obligated to observe the statutory provisions on data protection and not to disclose information obtained from the Client's domain to third parties or expose it to their access. Documents and data shall be secured against disclosure to unauthorized persons, taking into account the state of the art.
2. Furthermore, the Contractor shall oblige all persons entrusted by it with the processing and fulfillment of this DPA (hereinafter referred to as "employees") to maintain confidentiality (obligation to maintain confidentiality, Art. 28 Para. 3 lit. b GDPR). Upon request of the Client, the Contractor shall provide the Client with evidence of the obligation of the employees in writing or in electronic form.
3. The Contractor shall design its internal organization in such a way that it meets the special requirements of data protection. It undertakes to take all appropriate technical and organizational measures for the adequate protection of the Client Data pursuant to Art. 32 GDPR, in particular the measures listed in Annex 2 to this Agreement, and to maintain them for the duration of the processing of the Client Data.
4. The Contractor reserves the right to change the technical and organizational measures taken, while ensuring that the contractually agreed level of protection is not undercut.
5. At the request of the Client, the Contractor shall provide the Client with evidence of compliance with the technical and organizational measures.
6. The Contractor and the employees working for or on behalf of the Contractor shall be entitled to have the services to be rendered in accordance with the Main Contract and thus also the processing of personal data rendered from its head office, its business premises, branch offices or from the home and mobile office, provided that it is ensured that the protective measures defined in this DPA are complied with in this context.

## 4. Information and support obligations of the Contractor

1. In the event of disruptions, suspicion of data protection violations or violations of contractual obligations of the Contractor, suspicion of security-relevant incidents or other irregularities in the processing of the Client Data by the Contractor, persons employed by it within the scope of the DPA or by third parties, the Contractor shall inform the Client in writing or electronically without undue delay, but no later than within 48 hours. The same shall apply to audits of the Contractor by the data protection supervisory authority. These notifications should in each case contain at least the information specified in Art. 33(3) GDPR.
2. In the aforementioned case, the Contractor shall support the Client in the fulfillment of its educational, remedial and informational measures in this regard to the extent reasonable.
3. The Contractor undertakes to provide the Client, at the latter's request and within a reasonable period of time, with



all information and evidence required to carry out an inspection.

## 5. Other obligations of the Contractor

1. If the requirements of Art. 30 GDPR apply to the Contractor, the Contractor shall be obliged to keep a register of all categories of processing activities carried out on behalf of the Client pursuant to Art. 30 (2) GDPR. The directory shall be made available to the Client upon request.
2. The Contractor shall be obliged to support the Client in the preparation of a data protection impact assessment pursuant to Art. 35 GDPR and any prior consultation with the supervisory authority pursuant to Art. 36 GDPR.
3. The Contractor confirms that - insofar as there is a legal obligation to do so - it has appointed a data protection officer.
4. Should the Client Data at the Contractor be endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client thereof without undue delay, unless it is prohibited from doing so by court or administrative order. In this context, the Contractor shall immediately inform all competent bodies that the decision-making authority over the data lies exclusively with the Client as the "Responsible Party" within the meaning of the GDPR.

## 6. Subcontractor relationships

1. The Contractor may have the Processing of Personal Data performed in whole or in part by additional Processors (hereinafter "Subcontractors"). The Contractor shall inform the Client in text form in good time in advance about the commissioning of subcontractors or changes in the subcontracting. The Client may object to the subcontracting in text form within four weeks of becoming aware of it if there are objective reasons for doing so.
2. A subcontractor relationship within the meaning of these provisions shall not exist if the Contractor commissions third parties with services which are to be regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, guarding services, telecommunication services without any specific reference to services provided by the Contractor to the Client as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The obligation of the Contractor to ensure compliance with data protection and data security also in these cases shall remain unaffected.
3. The Contractor shall agree with the subcontractor on the content of the provisions made in this DPA. In particular, the TOM to be agreed with the subcontractor must provide an equivalent level of protection.
4. The Contractor has established subcontractor relationships with the companies listed in Annex 1, to which the Client agrees upon conclusion of this data processing agreement. The companies listed in Annex 1 may be amended by the Contractor, either by addition or removal. If the Contractor intends to add an additional subcontractor, they shall include the subcontractor in Annex 1 and inform the Client no later than four weeks before the intended use of the subcontractor. If the Client does not agree to the addition of the new subcontractor, they may object to the addition within four weeks after being notified. If the Client objects to the addition of the new subcontractor, the Contractor has the right to terminate the main agreement, including all annexes, within two weeks, provided that no alternative solution for continued cooperation can be found and the addition of the subcontractor is of particular importance to the Contractor's business.
5. The Contractor has concluded order processing agreements with the subcontractors in accordance with the requirements of Section 6 (3). The Client shall approve the aforementioned subcontractors upon this DPA becoming effective.
6. Part of the order processing agreements with the subcontractors is in particular that the subcontractors ensure that they have taken appropriate and suitable technical and organizational measures in accordance with Art. 32 GDPR for the processing of personal data carried out by them on behalf.



## 7. Control rights

1. The Client shall be entitled to regularly assure itself of compliance with the provisions of this DPA. For this purpose, it may, for example, obtain information from the Contractor, have existing test certificates from experts, certifications or internal audits presented to it or have the Contractor's technical and organizational measures inspected personally or by a competent third party during normal business hours, provided the third party is not in a competitive relationship with the Contractor.
2. The Client shall carry out inspections only to the extent necessary and take reasonable account of the Contractor's operating procedures. The Parties shall agree on the time and type of inspection in good time.
3. The Client shall document the results of the inspection and notify the Contractor thereof. In the event of errors or irregularities discovered by the Client, in particular during the inspection of order results, the Client shall inform the Contractor without delay. If facts are discovered during the inspection, the future avoidance of which requires changes to the ordered procedure, the Client shall inform the Contractor of the necessary procedural changes without delay.

## 8. Rights of Data Subjects

1. The Contractor shall support the Client as far as possible with suitable technical and organizational measures in fulfilling its obligations pursuant to Articles 12 to 22 and Articles 32 to 36 of the GDPR. The Contractor shall provide the Client with the requested information on Client Data without undue delay, but within 14 working days at the latest, unless the Client has the relevant information itself.
2. If the Data Subject asserts its rights pursuant to Articles 16 to 18 of the GDPR, the Contractor shall be obligated to correct, delete or restrict the Client Data without undue delay, at the latest within a period of 7 working days, upon instruction of the Client. The Contractor shall provide the Client with written evidence of the deletion, correction or restriction of the data upon request.
3. If a Data Subject asserts rights directly against the Contractor, such as the right to information, correction or deletion of his/her data, the Contractor shall forward this request to the Client and await the Client's instructions. The Contractor shall not contact the Data Subject without corresponding individual instructions.

## 9. Term

The term of this DPA corresponds to the term of the Main Contract. It thus ends automatically upon termination of the Main Contract. If the Main Contract can be terminated with due notice, the provisions on due notice of termination shall apply accordingly to this DPA. If the Contractor no longer processes any Client Data before the Main Contract expires, this DPA shall also end automatically.

## 10. Deletion and return after Termination

1. The Contractor shall return to the Client after termination of the Main Contract or at any time upon the Client's request all documents, data and data carriers provided to the Contractor or, at the Client's request, delete them completely and irrevocably, unless there is a statutory retention period. This shall also apply to copies of the Client Data at the Contractor's premises, such as data backups, but not to documentation that serves as proof of the proper processing of the Client Data in accordance with the order. Such documentation shall be kept by the Contractor for a period of 6 months and shall be returned to the Client upon request.



2. The Contractor shall confirm the deletion to the Client electronically. The Client shall have the right to control the complete and contractually compliant return or deletion of the data at the Contractor in an appropriate manner.
3. The Contractor shall be obligated to treat as confidential any data of which it becomes aware in connection with the Main Contract, even beyond the end of the Main Contract.

## 11. Liability

1. The liability of the Parties shall be governed by Art. 82 GDPR. Any liability of the Contractor towards the Client due to breach of obligations under this Agreement or the Main Contract shall remain unaffected.
2. The Parties shall each release themselves from liability if a Party proves that it is not responsible in any respect for the circumstance as a result of which the damage occurred to a Data Subject. This shall apply mutatis mutandis in the event of a fine imposed on a Party, whereby the indemnification shall be made to the extent that the respective other Party bears a share of the responsibility for the violation sanctioned by the fine.

## 12. Confidentiality & Data Secrecy

1. The Contractor undertakes to observe the same rules for the protection of secrets as are incumbent on the Client.
2. There shall be a duty of confidentiality for the Contractor's employees and third parties commissioned by the Contractor. The Contractor shall impose a written confidentiality obligation on the persons employed in the processing of Client Data pursuant to Art. 28 (3) lit. b GDPR. This is not necessary if the persons employed are already subject to an appropriate statutory duty of confidentiality. The Contractor shall document the obligation set forth in this clause in writing and submit it to the Client upon the Client's request.
3. The Contractor confirms that it is aware of the relevant data protection regulations. The Contractor warrants that it will familiarize the employees engaged in the performance of the work with the data protection provisions applicable to them and that it will oblige them to comply with the applicable data protection provisions. He shall monitor compliance with the data protection regulations.
4. The confidentiality obligations regulated in this clause shall continue to apply after termination of the contractual relationship.
5. Furthermore, in addition to the applicable statutory provisions (in particular § 3 German Telemedia-Telecommunication-Data Protection Act (TTDSG), § 203 German Criminal Code (StGB), §§ 4, 23 German Trade Secret Act (GeschGehG) and, if applicable, special professional confidentiality obligations), the Contractor shall also be obligated to keep secret and not disclose to third parties all information and data of which it becomes aware within the scope of the contractually agreed services (confidential information). Confidential information is in particular business and trade secrets, contract conclusions, technical or commercial information of any kind or other information which is designated as confidential or which by its nature is to be regarded as confidential. This also applies in particular to:
  - o Names, addresses as well as the personal, legal and economic circumstances of all customers of the Client and the personal, legal and economic circumstances of the Client and all other persons working for the Client.
  - o Information shall not be considered confidential if it was already publicly known at the time the information came to the knowledge of the Contractor. Likewise, information which has become publicly known or has been made publicly known at a later time with the consent of the Client shall not be regarded as confidential.
6. The Contractor undertakes to oblige all employees who gain knowledge of the aforementioned confidential information of the Client in the course of their work for the Client to do the same as he does himself.
7. If the Contractor commissions third parties, it shall ensure that the requirements of paragraphs 1 to 6 are implemented accordingly.



## 13. Final Provisions

1. The Parties agree that the defense of the right of retention by the Contractor within the meaning of § 273 of the German Civil Code (BGB) is excluded with respect to the data to be processed and the associated data carriers.
2. Amendments and supplements to this DPA must be made in electronic form.
3. In case of doubt, the provisions of this DPA shall take precedence over the provisions of the Main Contract. Should individual provisions of this DPA prove to be invalid or unenforceable in whole or in part or become invalid or unenforceable as a result of changes in legislation after the conclusion of the DPA, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision which comes as close as possible to the meaning and purpose of the invalid provision.
4. This DPA shall be governed by German law. The exclusive place of jurisdiction shall be the Contractor's registered office.

### Annexes

- **Annex 1** - Contract Specifications
- **Annex 2** - Technical & Organizational Measures (Art. 32 GDPR)



## Annex 1 - Contract Specifications

<b>Subject &amp; Term</b> Overview of Requirements and Specifications	
<b>(1) Main Contract</b>	IT Service Agreement
<b>(2) Subject</b>	IT services, in particular domain registration, allocation of IP addresses, DNS, web, server and email hosting, as well as SaaS services.
<b>(3) Purpose</b>	In order to fulfill the obligations of the Contractor arising from the Main Contract, personal data from the Client's sphere of control shall be processed by the Contractor to the full extent within the meaning of Art. 4 No. 2 of the GDPR, in particular collected, stored, changed, read out, queried, used, disclosed, compared, linked and deleted as necessary in each case. The purpose of the processing thus depends on the respective order described in the main contract
<b>(4) Art der Daten</b>	<p>The categories of personal data concerned by the processing depend on the use of the Contractor's services by the Client. The categories of data that may be considered as the subject of processing are as follows:</p> <ul style="list-style-type: none"><li>• Master data (e.g. names, addresses, dates of birth),</li><li>• Contact data (e.g. e-mail addresses, telephone numbers),</li><li>• Content data (e.g. photographs, videos, content of documents),</li><li>• Contract data (e.g. subject matter of contract, terms, customers),</li><li>• Payment data (e.g. bank details, payment service providers),</li><li>• Usage data (e.g. course of web services, access times),</li><li>• Connection data (e.g. device ID, IP addresses, URL referrers), and</li><li>• Location data (e.g. GPS data, IP geolocation).</li></ul>
<b>(5) Data Subject</b>	<p>The categories of data subjects concerned by the processing depend on the use of the Contractor's services by the Client. The categories of data subjects that may be considered are:</p> <ul style="list-style-type: none"><li>• Employees</li><li>• Apprentices and Trainees</li><li>• Applicants</li><li>• Former Employees</li><li>• Freelancers</li><li>• Shareholders, Corporate Bodies of the Company</li><li>• Relatives of Employees</li><li>• Customers / Interested Parties</li><li>• Suppliers and Service Providers</li><li>• Tenants</li><li>• Business Partners</li><li>• External Consultants</li><li>• Visitors</li><li>• Press Representatives</li></ul>



## Subcontractors

No.	Name of Subcontractor Address / Country	Subject of Service	Processed Data
1	Cloudflare, Inc. 101 Townsend Street San Francisco, CA 94107 USA	All Services	See above „Type“
2	Stripe Payments Europe, Limited 1 Grand Canal Street Lower Grand Canal Dock D02 H210, Dublin Ireland	All Services	See above „Type“
3	Intercom R&D Unlimited Company 124 St Stephen's Green DC02 C628, Dublin 2 Ireland	All Services	See above „Type“
4	sevDesk GmbH Im unteren Angel 1 77652 Offenburg Germany	All Services	See above „Type“
5	OpenAI Ireland Ltd 1st Floor, The Liffey Trust Centre 117-126 Sheriff Street Upper D01 YC43, Dublin 1 Ireland	AI-Services	See above „Type“
6	NETIM SARL 264 avenue Arthur Notebart 59160 Lille France	Hosting-Services / Domains	See above „Type“
7	Google Cloud EMEA Limited 70 Sir John Rogerson's Quay D02 R296, Dublin 2 Ireland	All Services	See above „Type“
8	Twilio Ireland Limited 70 Sir John Rogerson's Quay D02 R296, Dublin 2 Ireland	All Services	See above „Type“
9	WhatsApp Ireland Limited Merrion Road D04 X2K5, Dublin 4 Ireland	All Services	See above „Type“
10	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Germany	Hosting-Services	See above „Type“
11	The Constant Company, LLC 319 Clematis St West Palm Beach, FL 33401 USA	All Services	See above „Type“

**Anschrift / Address**  
Gentlent GmbH  
Am Trippelsberg 92  
40589 Düsseldorf  
Germany

**Kontakt / Contact**  
E-Mail: support@gentlent.com  
Tel.: +49 (0) 211 86843 - 0  
Fax: +49 (0) 211 86843 - 999  
Web: <https://www.gentlent.com>

**Rechtliches / Legal Details**  
Amtsgericht Düsseldorf  
HR-Nr.: HRB 103552  
USt.-ID: DE366296666  
CEO: Tom Klein, Florian Oliver Elke

**Bankkonto / Bank Account**  
SOLARIS SE  
IBAN: DE71 1101 0101 5786 2498 11  
BIC: SOBKDEB2XXX



## Annex 2 - Technical & Organizational Measures

Pursuant to Article 32 of the GDPR, data controllers are obliged to take technical and organizational measures to ensure the security of the processing of personal data. Measures must be selected in such a way that, taken together, they ensure an appropriate level of protection. Against this background, this overview explains which concrete measures have been taken by the Contractor with regard to the processing of personal data in the specific case.

### Instructions to Technical & Organizational Measures

#### 1. Organisation of Information Security

Policies, processes and responsibilities must be defined to implement and control information security.

Measures:

- Information security policy.
- User guidelines for handling devices and behavior when using information technology.
- Processes for the management of data media and disposal of data media.
- Definition of roles and responsibilities for application and system operation, data protection, and information security.
- Obligation of employees to maintain confidentiality and data secrecy.
- Regular implementation of training and awareness measures.

Further Measures:

#### 2. Privacy by Design

Privacy by design includes the idea that systems should be designed and constructed in such a way that the amount of personal data processed is minimized. Essential elements of data economy are the separation of personal identifiers and content data, the use of pseudonyms, and anonymization. In addition, the deletion of personal data must be implemented in accordance with a configurable retention period.

Measures:

- No more personal data is collected than is necessary for the respective purpose.
- Process to ensure privacy by design when introducing or modifying systems and applications.
- The processing operations and systems are designed in such a way that they enable and ensure DSGVO-compliant deletion of the personal data processed.

Further Measures:

#### 3. Privacy by Default

Privacy by Default refers to the privacy-friendly default settings / standard settings. To what extent have these been made by you? Example: When visiting a website, the visitor can expect that all programs that collect personal data are initially deactivated.

Measures:

- Simple exercise of the right of withdrawal of the data subject by technical measures.
- Tracking functions that monitor the data subject are disabled by default.
- All default settings for selection options meet the requirements of the GDPR with regard to privacy-friendly default settings (e.g., no default settings for opt-ins).

Further Measures:

#### 4. Access Control

Measures to ensure that those authorized to use the data processing procedures can only access the personal data or information and data requiring protection that are subject to their access authorization (description of security mechanisms inherent in the system, encryption procedures in accordance with the state of the art. In the case of online access, it must be made clear which side is responsible for issuing and managing access security codes). The Contractor shall ensure that the users authorized to use IT

**Anschrift / Address**  
Gentlent GmbH  
Am Trippelsberg 92  
40589 Düsseldorf  
Germany

**Kontakt / Contact**  
E-Mail: support@gentlent.com  
Tel.: +49 (0) 211 86843 - 0  
Fax: +49 (0) 211 86843 - 999  
Web: <https://www.gentlent.com>

**Rechtliches / Legal Details**  
Amtsgericht Düsseldorf  
HR-Nr.: HRB 103552  
USt.-ID: DE366296666  
CEO: Tom Klein, Florian Oliver Elke

**Bankkonto / Bank Account**  
SOLARIS SE  
IBAN: DE71 1101 0101 5786 2498 11  
BIC: SOBKDEB2XXX



infrastructure can only access content for which they are authorized and that personal data cannot be copied, modified or deleted without authorization during processing and after storage.

Measures:

- Authorization concepts documented.
- Avoidance of group users.
- Access to data is restricted and only possible for authorized persons.
- Blocking of the user account in case of failed attempts / inactivity.
- Locking of the terminal device when leaving the workplace or inactivity.
- Number of administrators reduced to the "bare minimum".
- Logging of accesses to applications, especially when entering, changing, and deleting data.
- Implementation of a process for assigning authorizations.
- Regular review of authorizations.
- Password policy, implementation of complex passwords.
- Use of strong authentication with at least 2 factors from knowledge, possession, properties (pin, token, smartcard, biometric methods).

Further Measures:

### 5. Cryptographie and Pseudonymization

Use of encryption procedures to ensure the proper and effective protection of the confidentiality, authenticity or integrity of personal data or information requiring protection. Measures that are likely to make identification of the data subject difficult.

Measures:

- Organizational instruction for the encryption of data.
- Encryption of data carriers (e.g. mobile hard disks, USB sticks, etc.).
- Encryption of end devices (PC, laptop, smartphones).
- Encrypted storage of personal data.
- Encryption of data backup media (e.g., tapes, hard disks, etc.).
- Encryption of network access points and connections.
- Use of pseudonyms, procedures for pseudonymization of data.
- Use of procedures for anonymizing data.

Further Measures:

### 6. Building protection

Preventing unauthorized physical access to, damage to and impairment of the organization's information and information processing equipment. The Contractor shall take measures to prevent unauthorized persons from gaining access (to be understood spatially) to data processing equipment with which personal data are processed.

Measures:

- Zone concept and definition of security areas.
- Building security by means of fences.
- Security locks and key management / logging of key issuance.
- Use of locking and access systems (chip card / transponder locking system, code security, etc.).
- Alarm system.
- Video surveillance.
- Light barriers / motion detectors.
- Use of security guards.
- Employee / visitor passes.
- Regulation for dealing with visitors.
- Registration for visitors (reception).
- Control of visitors (gatekeeper/reception).
- Logging of visitors (visitor book).

Further Measures:

Further measures have been implemented by our service providers. If you are interested in the specific technical and organizational measures taken by the service providers, please feel free to contact us.



## 7. Protection of operating resources / information assets

Prevention of loss, damage, theft or impairment of assets and disruption of the organization's operations.

Measures:

- Secure placement of the systems so that protection against theft is guaranteed.
- Protection of operating equipment against fire, water, or overvoltage.
- Storage of files and documents in locked offices, filing cabinets.
- Placement of server and network components in secured rooms, cabinets, etc.
- Regular maintenance of operating equipment.
- Secure deletion, destruction, and disposal of operating equipment.

Further Measures:

Further measures have been implemented by our service providers. If you are interested in the specific technical and organizational measures taken by the service providers, please feel free to contact us.

## 8. Operating procedures and responsibilities

Ensure proper and secure operation of systems and procedures for processing information.

Measures:

- Documented system configurations and operating procedures, operations management manuals.
- Clear assignment of responsibilities for system and application support.
- Separation of processing of data from the individual clients.
- Separation of development, test, and production systems.
- Monitoring of system operation and installations.
- Maintenance contracts with appropriate response time.
- Use of systems for managing systems and devices (asset management, mobile device management, software management and distribution).

Further Measures:

## 9. Data backups

Measures to ensure that personal data or information and data requiring protection are protected against accidental destruction or loss.

Measures:

- Data backup concept with regular backups.
- Outsourcing of backups to other fire zones.
- Outsourcing of backups to other buildings.
- Regular testing of data backup and recovery of data, applications, and systems.

Further Measures:

## 10. Malware protection and patch management

Preventing exploitation of technical vulnerabilities by using up-to-date antivirus software and implementing patch management.

Measures:

- Regular monitoring of the status of security updates and system vulnerabilities.
- Use of anti-malware software.
- Regularly apply security patches and updates.

Further Measures:

## 11. Logging and monitoring

Measures to ensure that it is possible to check and determine retrospectively whether and by whom personal data has been entered into, modified or removed from IT systems. (All system activities are logged; the logs are kept by the contractor for at least 3 years).

Measures:

**Anschrift / Address**  
Gentlent GmbH  
Am Trippelsberg 92  
40589 Düsseldorf  
Germany

**Kontakt / Contact**  
E-Mail: support@gentlent.com  
Tel.: +49 (0) 211 86843 - 0  
Fax: +49 (0) 211 86843 - 999  
Web: <https://www.gentlent.com>

**Rechtliches / Legal Details**  
Amtsgericht Düsseldorf  
HR-Nr.: HRB 103552  
USt.-ID: DE366296666  
CEO: Tom Klein, Florian Oliver Elke

**Bankkonto / Bank Account**  
SOLARIS SE  
IBAN: DE71 1101 0101 5786 2498 11  
BIC: SOBKDEB2XXX



- Logging of system administrator activities.
- Monitoring of system usage.
- Logging of accesses.
- Logging of accesses.
- Evaluation of log files.

Further Measures:

Further measures have been implemented by our service providers. If you are interested in the specific technical and organizational measures taken by the service providers, please feel free to contact us.

## 12. Network Security Management

Adequate protection for the network must be implemented so that the information and infrastructure components are protected.

Measures:

- Use of network management software.
- Use of firewall systems.
- Use of intrusion detection / intrusion prevention systems.
- User authentication and encryption of external access.

Further Measures:

Further measures have been implemented by our service providers. If you are interested in the specific technical and organizational measures taken by the service providers, please feel free to contact us.

## 13. Information transfer

Measures to ensure that personal data or information requiring protection and data cannot be read, copied, modified or removed by unauthorized persons during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and determine to which bodies a transmission of personal data or information requiring protection and data is intended by data transmission facilities. (Description of the facilities and transmission protocols used, e.g. identification and authentication, encryption in accordance with the state of the art, automatic call-back, etc.).

Measures:

- Regulations for the exchange of sensitive information and restriction of the group of persons authorized to transfer data.
- Transfer of data to third parties only after verification of the legal basis.
- Legality and written definition of the transfer of data to third countries.
- Secure data transmission between client and server.
- Appropriate protection of e-mails containing sensitive information/data.
- Use of encrypted external access.
- Secure transport and dispatch of data carriers, data, and documents.

Further Measures:

## 14. Mains disconnection

Groups of information services, clients, users and information systems should be kept separate from each other in networks.

Measures:

- Logical client separation.
- Data separation by segmenting networks of different clients.
- Separation of networks for remote accesses.

Further Measures:

## 15. Acquisition, development and maintenance of systems

Measures to ensure that information security is an integral part across the lifecycle of information systems.

Measures:

- Definition of security-specific regulations and requirements for the deployment of new information systems and for the expansion



- of existing information systems.
- Definition of regulations for the development and adaptation of software and systems.
  - Guidelines for secure system development.
  - Monitoring of outsourced system development activities.
  - Protection of test data.

Further Measures:

### 16. Supplier Relations

Measures concerning information security to reduce risks related to suppliers' access to the company's assets should be agreed with sub-suppliers / subcontractors and documented.

Measures:

- Selection of the contractor under due diligence aspects (in particular with regard to data security).
- Written instructions to the contractor (e.g., by order processing agreement) within the meaning of the GDPR the contractor has appointed a data protection officer.
- Effective control rights vis-à-vis the contractor agreed.
- Prior review and documentation of the security measures taken at the contractor.
- Obligation of the contractor's employees to maintain data secrecy.
- Ongoing review of the contractor and its activities.
- Ensuring the destruction of data after completion of the order.

Further Measures:

### 17. Information security incident management

Consistent and effective measures for the management of information security incidents (theft, system failure, etc.) shall be implemented.

Measures:

- Documented procedure for handling security incidents.
- Immediate information of the client in the event of data protection incidents.
- Involvement of the data protection and information security officer in the event of data protection incidents.
- Formal process and responsibilities for the follow-up of security incidents and data breaches.

Further Measures:

### 18. Information security aspects of business continuity management / emergency management

Maintaining system availability in difficult situations, such as crisis or damage events. Emergency management must ensure this. The requirements regarding information security should be defined in the planning for business continuity and disaster recovery.

Measures:

- Use of redundant systems.
- Use redundant systems at physically separate locations (e.g., emergency data center).
- Documented emergency plans.
- Regular tests regarding the effectiveness of the emergency measures.
- Early information of the customer in case of emergencies.

Further Measures:

Further measures have been implemented by our service providers. If you are interested in the specific technical and organizational measures taken by the service providers, please feel free to contact us.

### 19. Compliance with legal and contractual requirements

Implementation of measures to prevent violations of legal, official or contractual obligations as well as any safety requirements.

Measures:

- Ensuring compliance with legal obligations within the scope of the cooperation.
- Returning all data, operating resources, and information assets to the client at the end of the contract.



- Establishment of license management.
- Confidentiality obligations with employees as well as subcontractors and service providers.

Further Measures:

## 20. Data protection requirements and data protection management

Privacy as well as protection of personal data should be ensured according to the requirements of relevant legal regulations, other regulations as well as contractual provisions.

Measures:

- Establishment of a data protection organization.
- Appointment of a data protection officer.
- Directory of processing activities.
- Data protection impact assessment for processes that handle sensitive information/data.
- Conducting data protection training.
- Establishment of a data protection management system.
- Documented data protection concept.
- Data protection guidelines implemented.

Further Measures:

## 21. Information Security Audits

Regular checks must be made to ensure that information processing is carried out in accordance with the defined security measures. For this purpose, the Contractor shall perform regular audits. The Contractor grants the Client the right to carry out regular audits / checks at its premises.

Measures:

- Regular performance of internal audits on the topics of data privacy and information security.
- Conducting penetration tests.

Further Measures: