### **Agreement on data processing**

### **according to Art. 28 GDPR**

|  |
| --- |
| **[COMPANY]** |

- as the person responsible, hereinafter referred to as the client -

and

**Elara Digital GmbH, Spandauer Damm 71, 14059 Berlin**

- as the processor, hereinafter referred to as contractor -

**Preamble
Aim of this agreement**

The client has commissioned the contractor to provide services in the area of "Software as a Service" and hosting.

This agreement on commissioned processing (hereinafter referred to as "Agreement") specifies the obligations of the contracting parties under data protection law, which arise in particular from Art. 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).

It applies to all activities in which the contractor or subcontractors (subcontractors) commissioned by the contractor and previously approved by the client process the client's personal data or may come into contact with such data. Insofar as the term "data" is used in the following, in case of doubt, this refers to the client's personal data.

**§ 1
Subject matter and duration of the agreement
(on Art. 28 para. 3 GDPR)**

The subject matter and duration of the order are determined in full by the information provided in the respective contractual relationship. Based on this contract, the contractor processes personal data for the client within the meaning of Art. 4 No. 2 and Art. 28 GDPR.

**§ 2
Scope, type and purpose of the commissioned processing, type of data, group of data subjects
(on Art. 28 (3) GDPR)**

* 1. Description of the processing operation (Art. 4 No. 2 GDPR)

Nature and purpose of processing

|  |
| --- |
| The processing of personal data by the contractor takes place within the scope of and serves to enable the use of the software offered by the client and its employees. |

* 1. Type of personal data (Art. 4 No. 1 GDPR):

|  |
| --- |
| Customer data* + Name (first name, surname)
	+ Telephone number
	+ e-mail address
	+ Profile picture
	+ Comments

Employee data of the customer* + Name (first name, surname)
	+ Telephone number
	+ e-mail address
	+ Profile picture
	+ Comments
 |
|  |

* 1. Categories of data subjects:

|  |
| --- |
| * Customer
* Employee of the customer
 |

**§ 3
Instructions and powers to issue instructions
(on Art. 28 para. 3 lit. a, 29 GDPR)**

* 1. The Contractor shall process the Client Data only within the scope of the assignment and exclusively on behalf of and by the instructions of the Client within the meaning of Art. 28 GDPR (order processing); this applies in particular about the transfer of personal data to a third country or an international organisation. In this respect, the client has the sole right to issue instructions regarding the type, scope and method of processing activities (hereinafter referred to as the "right to issue instructions"). If the Contractor is obliged by the law of the European Union or the Member States to which it is subject to carry out further processing, it shall inform the Client of these legal requirements before processing.
	2. Instructions shall always be issued by the Client in writing; the Client shall confirm verbal instructions in text form. If the Contractor thinks that an instruction from the Client violates data protection regulations, it must inform the Client immediately. The Contractor shall be entitled to suspend the execution of the instruction in question until it has been confirmed or amended by the Client.

**§ 4
Technical and organizational measures, Data protection and data security concept
(on Art. 28 para. 3 lit. c GDPR)**

* 1. The Contractor is obliged to observe the statutory provisions on data protection and not to disclose the information obtained from the Client's area to third parties or expose it to their access. Documents and data must be secured against unauthorized access, considering the state of the art. The client shall demonstrate compliance with the obligations set out in this contract by suitable means.
	2. Furthermore, the Contractor shall oblige all persons entrusted by it with the processing and fulfillment of this contract (hereinafter referred to as "employees") to maintain confidentiality in writing (Art. 28 para. 3 lit. b GDPR) and ensure compliance with this obligation with due care. At the Client's request, the Contractor shall provide the Client with evidence of the employees' obligation 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. The Contractor undertakes to take all appropriate technical and organizational measures to adequately protect the Client Data by Art. 32 GDPR, in particular, the measures listed in Annex 1 to this Agreement, and to maintain these for the duration of the processing of the Client Data.
	4. The Contractor reserves the right to change the technical and organizational measures taken, ensuring that the contractually agreed level of protection is not undercut. The Contractor shall inform the Client immediately in writing if it has reason to believe that the measures by Annex 1 are no longer sufficient and shall consult with the Client regarding further technical and organizational measures.
	5. At the request of the Client, the Contractor shall provide the Client with suitable evidence of compliance with the technical and organizational measures specified in Annex 1.

**§ 5
Obligations of the contractor
(on Art. 28 para. 3 lit. b, e, f GDPR)**

* 1. In the event of disruptions, suspected data protection violations or breaches of contractual obligations of the Contractor, suspected security-related incidents or other irregularities in the processing of the Client Data by the Contractor, persons employed by the Contractor within the scope of the order or by third parties, the Contractor shall inform the Client immediately, but at the latest within 48 hours of becoming aware of this, in electronic form. The date of receipt by the Client shall be decisive for compliance with the deadline. The same applies to contractor audits by the data protection supervisory authority. The notifications shall contain at least the information specified in Art. 33 (3) GDPR.
	2. In the aforementioned cases, the Contractor shall support the Client in fulfilling its relevant clarification, remedial and information measures within the reasonable scope. In particular, the Contractor shall immediately take the necessary measures to secure the data and mitigate possible adverse consequences for the data subjects, inform the Client thereof, and request further instructions from the Client.
	3. The Contractor undertakes to provide the Client with all information and evidence required to inspect by § 7 of this contract within a reasonable period upon the Client's verbal or written request. Furthermore, at the Client's request, the Contractor shall provide the Client with a comprehensive and up-to-date data protection and security concept for order processing and authorized persons.
	4. At the client's request, the contractor must keep a list of all categories of processing activities carried out on behalf of the client by Art. 30 para. 2 GDPR. The list must be made available to the client upon request.
	5. The contractor must support the client in preparing a data protection impact assessment by Art. 35 GDPR and any prior consultation with the supervisory authority by Art. 36 GDPR.
	6. The Contractor confirms that it has appointed a data protection officer insofar as there is a legal obligation to do so. The full contact details of the data protection officer shall be provided to the Client in text form upon conclusion of the contract. A change in the person of the company data protection officer/contact person for data protection must be communicated to the client immediately in writing.
	7. Should the Client Data be jeopardized at the Contractor by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client of this immediately, unless it is prohibited from doing so by court or official 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 "controller" within the meaning of the GDPR.
	8. All client data is stored in a suitable form so that it can be clearly identified and not be mixed with other clients.

**§ 6
Subcontracting relationships
(on Art. 28 para. 2, para. 3 lit. d, para. 4 GDPR)**

* 1. Within the scope of its contractual obligations, the Contractor is not authorized to establish subcontracting relationships with subcontractors ("**subcontractor relationship**"). Exceptions are only permitted with the prior express written consent of the Client in individual cases; this is deemed to have been granted for the subcontractors named in Annex 2. In any case, the Contractor shall ensure that the provisions agreed in this contract also apply to the subcontractors commissioned by it, whereby the Client shall be granted all control rights vis-à-vis the subcontractor by this contract. Subcontractor relationships with third parties outside the European Economic Area are not permitted.
	2. A subcontractor relationship within the meaning of these provisions does not exist if the contractor commissions third parties with services that are to be regarded as purely ancillary services. These include, for example, postal, transportation and shipping services, cleaning services, security services, and telecommunications services with no specific connection to services that the contractor provides for 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 Contractor's obligation to ensure data protection and security compliance in these cases remains unaffected.

**§ 7
Control rights of the client, toleration and cooperation obligations of the contractor
(on Art. 28 para. 3 lit. h GDPR)**

* 1. The Client shall be entitled to verify compliance with all data protection regulations and agreements made, in particular the technical and organizational measures taken by the Contractor (see Annex 1), before the start of data processing and after that regularly. The Client may also have this inspection carried out by a third party. The Contractor may provide evidence in individual cases by complying with approved rules of conduct under Art. 40, 41 GDPR or using a suitable and approved certification procedure under Art. 42 GDPR.
	2. The Client shall only carry out inspections to the extent necessary and reasonably consider 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 inspection results and inform the Contractor thereof. In the event of errors or irregularities that the client discovers, particularly during the inspection of order results, it must inform the contractor immediately. Suppose facts are discovered during the inspection that require changes to the ordered process flow to avoid them in the future. In that case, the client shall inform the contractor of the necessary procedural changes without delay.

**§ 8
Return of data carriers provided and deletion of data stored by the contractor after the termination of the contract
(on Art. 28 para. 3 lit. g GDPR)**

* 1. The Contractor shall return to the Client all documents, data and data carriers provided to it after the termination of the main contract or at any time at the Client's request, or delete them completely and irrevocably at the Client's request unless there is a statutory retention period. This also applies 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 returned by the Contractor to the Client upon request.
	2. The Contractor shall confirm the deletion to the Client in writing. The Client shall have the right to check the complete and contractually compliant return or deletion of the data at the Contractor's premises in a suitable manner.

**§ 9
Place of processing
(on Art. 28 para. 3 lit. a GDPR)**

The processing and use of the data shall take place exclusively 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, provided that the latter has decided to apply the GDPR. Any relocation to a third country requires the prior written consent of the client. The client is not obliged to give its consent. It is free to make its own decision in this regard. The Contractor shall ensure that the special legal requirements are met during transfer to a third country (Art. 44 et seq. GDPR).

**§ 10
Termination of contract**

The term of this agreement corresponds to the term of the main contract. If the main contract ends due to an ordinary or extraordinary termination agreement, this agreement shall also end. Isolated termination of this agreement without termination of the main contract is not permitted.

**§ 11
Liability**

The parties' liability shall be governed by Art. 82 GDPR. Any liability of the Contractor towards the Client for breach of obligations under this contract or the main contract shall remain unaffected by this.

**§ 12
Final provisions**

* 1. Amendments and supplements to this agreement must be made in writing. This also applies to any deviation from this written form requirement. Amendments and supplements require express reference to the fact that they constitute an amendment or supplement to these terms and conditions.
	2. Should a provision of this agreement be invalid, this shall not affect the validity of the remaining provisions. The parties undertake to replace the invalid provision with a valid provision that comes as close as possible to the invalid provision.
	3. German law shall apply. The place of jurisdiction shall be determined by the provisions in the main contract.

**Appendix 1**

**Data protection and data security concept**

1. **Confidentiality (Art. 32 (b) GDPR)**
2. **Access control**

*Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data is processed or used.*

1. **Measures at the company headquarters**

|  |  |
| --- | --- |
| Alarm system with connection to security service or police | Written regulations on access authorization |
| Automatic access control system | Manual locking system |
| Chip cards / transponder systems | Security locks |
| Biometric access locks | Reception / Reception / Porter |
| List of issued keys/transponders is kept | Employee ID cards must be carried |
| Locking system with code lock | Video surveillance |
| Visitors' book / Visitors' log | Visitor passes are issued |
| Work areas and areas accessible to visitors are separated from each other | Visitors have access to all areas of the building |
| Access for visitors only with a confidentiality agreement | Visitors accompanied by employees for the entire duration of their visit |
| Careful selection of external service providers who are granted access to the building (security staff, cleaning services, tradesmen, etc.) | All external service providers (security staff, cleaning services, tradesmen, etc.) must sign a confidentiality agreement before entering the building for the first time |
| Written rules for the selection and review of external service providers | Further measures: |

1. **Measures regarding server rooms**

|  |  |
| --- | --- |
| Alarm system with connection to security service or police | Written regulations on access authorization |
| Automatic access control system | Manual locking system |
| Chip cards / transponder systems | Security locks |
| Biometric access locks | Server rooms demarcated (restricted area) |
| List of issued keys/transponders are kept | Number of people allowed to enter server rooms limited to a minimum |
| Locking system with code lock | Video surveillance |
| No granting of access authorizations for visitors | Further measures |

1. **Access control**

*Measures that are suitable for preventing data processing systems from being used by unauthorized persons.*

|  |  |
| --- | --- |
| Written regulations for granting user accounts available | Logging the allocation and withdrawal of user accounts |
| Granting of user accounts only by administrators | Only personalized user accounts |
| Login with biometric data | Login with user name + password |
| Password security policy in place (minimum requirement for password length and complexity) | Compliance with the password security policy is technically enforced |
| Regular password change required | Access block for unsuccessful login attempts |
| Logging of unsuccessful login attempts | Automatic screen lock |
| Employees must lock their desktop when leaving the workplace | Data protection and data security policy in place, currently being drafted |
| Anti-virus software for servers | Anti-virus software for clients |
| Anti-virus software for mobile devices | Firewall |
| Any anti-virus software and firewall used is updated regularly | Intrusion Detection Systeme |
| Mobile Device Management | Mobile Device Policy |
| Enclosure lock | Use of VPN for remote access |
| Encryption of notebooks / tablets*Bitlocker, FileVault.* | Encryption of data carriers*Bitlocker, FileVault.* |

1. **Access control**

*Measures that ensure that persons authorized to use a data processing system can only access the data subject to their access authorization.*

|  |  |
| --- | --- |
| User authorization concept in place | Minimum number of administrators |
| Logging of assignment and revocation of authorizations | Authorizations only granted by administrators |
| Granting of access rights according to the need-to-know principle | Granting of differentiated authorizations (e.g. read-only, read-and-write, ...) |
| Creation of user profiles | Regular review of the authorizations granted  |
| Logging of attempted and successful access to applications and/or data | Policy for secure deletion/destruction of data carriers no longer in use |
| Data carrier management (regulation of output; prohibition of the use of own data carriers) | Further measures: |

1. **Separation control**

*Measures to ensure that data collected for different purposes can be processed separately.*

|  |  |
| --- | --- |
| Separation of production and test environments | Separation of data from different controllers |
| Physical separation | Logical separation |
| Separation via authorization concept | Further measures: |

1. **Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)**

*The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.*

|  |  |
| --- | --- |
| Pseudonymization of data is possible if required | Personal data is pseudonymized as quickly as possible |
| Separation of the assignment data to remove the pseudonymization in a separate and secure system | Personal data is anonymized (it is impossible to assign it to a person again, regardless of the effort involved) |
| Pseudonymization can only be removed if there is a legal basis and only for individual employees who have been specially trained in data protection law | Further measures: |

1. **Integrity (Art. 32 (b) GDPR)**
2. **Transfer control**

*Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data carriers and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.*

|  |  |
| --- | --- |
| E-mails containing personal data are sent exclusively in encrypted form | Provision of personal data only via encrypted connections |
| Dispatch of data carriers (paper or electronic) by post, courier, etc. | Careful selection of transport personnel and vehicles |
| Use of secure transport containers | Documentation of data recipients and the duration of the planned transfer or the agreed deletion periods |
| Forwarding of data only in anonymized form | Forwarding of data only in pseudonymized form |
| Use of VPN for remote access | Logging every time data is retrieved |
| Logging of regular retrieval and transmission processes | Remote maintenance of systems in which the controller's personal data is stored |
| Blocking of external interfaces (e.g. USB) | Clean-Desk-Policy |
| Data protection safe available | Policy for the deletion and destruction of data carriers |
| File shredder | External document shredderProvider: Shred-IT |

1. **Input control**

*Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, modified or removed from data processing systems.*

1. The Contractor processes the Client's personal data primarily on the Client's IT systems. For these processing operations, no input control information is required from the Contractor. With regard to input control, the following technical and organizational measures of the client apply, for the implementation and maintenance of which the client is responsible:
* The entry, modification and deletion of personal data is tracked by means of audit-proof logging in the respective applications.
* Detailed authorization concepts for the applications are implemented in the system and any changes made are documented in the ticket system.
* The activities carried out are logged and the logs are checked regularly.
* By monitoring log files, those responsible are technically alerted in the event of critical operations.
1. Insofar as the personal data of the Client is processed on the Contractor's IT systems in individual cases, e.g. through transmitted screenshots of error messages or test databases or similar, this is done exclusively for analysis purposes. This data is not transmitted back to the client in modified form for further use but is deleted by the contractor after the analysis has been completed. No separate measures for input control are therefore required for this data; however, the measures listed above under A. 1. to 4. ensure that only authorized persons at the Contractor can access this data and that access can be traced.
2. **Availability and resilience of systems and services (Art. 32 (b), (c) GDPR)**
3. **Availability control**

*Measures to ensure that personal data is protected against accidental destruction or loss.*

1. **General measures**

|  |  |
| --- | --- |
| Use of a spam filter | Written backup and recovery concept |
| Automatic regular data backup | Reasonably frequent backup of data |
| Storage of backup media in a secure location | Storage time for backups regulated in writing |
| Fire and smoke detection systems | Uninterruptible power supply |
| Retention period for backups depends on the deletion period of the backed-up data | Further measures: |

1. **Measures regarding server rooms**

|  |  |
| --- | --- |
| Fire and smoke detection systems | Moisture monitoring |
| Temperature monitoring | Protective socket strips |
| Air conditioning  | Uninterruptible power supply |
| Hard disk mirroring | Alarm message in the event of unauthorized access |
| No sanitary connections in or above the server room | Separate partitions for operating systems and data |
| Existence of an emergency plan (e.g. BSI IT-Grundschutz 100-4) | Further measures: |

1. **Rapid recoverability (Art. 32 para. 1 lit. c GDPR)**

*Measures to ensure that data can be restored quickly in the event of accidental destruction or accidental loss.*

|  |  |
| --- | --- |
| Regular data recovery tests | Logging the results of the data recovery tests |
| Further measures: |  |

1. **Procedures for regular review, assessment and evaluation of the effectiveness of the TOMs to ensure the security of processing (Art. 32 (d) GDPR)**
2. **Data protection management (Art. 25 para. 1 GDPR)**

*Measures to ensure that all data protection requirements are always met.*

|  |  |
| --- | --- |
| Software solutions for data protection management in use | Written data protection and data security concept in place |
| Central documentation of all procedural instructions and regulations on data protection, available to employees at any time (as required/authorized) | At least annual review of the effectiveness of the protective measures; if necessary, the protective measures are adjusted |
| Documentation of the review of the effectiveness of the protective measures | Certification available |
| Existence of a processing directory in accordance with Art. 30 para. 2 GDPR - Currently still in progress | Regular review and updating of the processing directory-  |
| Regular training of all employees (data protection and data security) | All employees are bound to confidentiality/data secrecy or are subject to a legal duty of confidentiality |
| If required by law, the data protection impact assessment is carried out in accordance with Art. 35 GDPR | Further measures: |

1. **Incident-Response-Management**

*Measures to ensure a rapid and appropriate response to security breaches.*

|  |  |
| --- | --- |
| Process for detecting and reporting security incidents and potential data protection breaches | Formal process and clear regulation of responsibilities for the follow-up of security incidents and data protection violations |
| Regular checks of the selected files / logged attack attempts for automated protection installations | Documentation of all security incidents and data protection breaches |
| Regulation of responsibility for reporting security incidents and data protection breaches to the controller | Further measures: |

1. **Data protection-friendly default settings (Art. 25 para. 2 GDPR)**

*Measures to ensure that the principles of privacy by design and privacy by default are complied with.*

|  |  |
| --- | --- |
| No more personal data is collected than is necessary for the respective purpose | Simple exercise of data subject rights possible |
| Automatic deletion of data ensured once the purpose no longer applies | Further measures: |

1. **Order control**

*Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.*

|  |  |
| --- | --- |
| Careful selection of subcontractors with regard to data protection and data security | Written rules on what must be observed when selecting subcontractors |
| Documentation of the selection process | Authority to issue instructions is clearly defined |
| Conclusion of the necessary contracts (order processing contract or standard contractual clauses) is ensured by appropriate guidelines | Data processing agreements comply with the requirements of Art. 28 GDPR |
| Agreement of on-site inspections at the subcontractor | Ongoing, regular review of the sub-provider and its level of protection |
| The use of other service providers by the subcontractor is prevented | The subcontractor may, in turn, use other service providers |
| All requirements from the data processing agreement with the controller are also contractually agreed with the subcontractor | Further measures: |

**Appendix 2**

**List of subcontractors**

|  |  |  |
| --- | --- | --- |
| **Subcontractor** | **Address / Country** | **Service** |
| Microsoft | Unter den Linden 17, 10117 Berlin | Server-Hosting, Azure-Blob Storage |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Assessment of US data transfers Microsoft:**

**Risks arising from US security regulations:** Foreign Intelligence Surveillance Act (FISA), Section 702: Under Section 702 of FISA, the United States government may compel "providers of electronic communication services" to disclose information about non-U.S. citizens located outside the United States in order to obtain information for foreign intelligence purposes. EO 12333 and Presidential Policy Directive 28 ("PPD-28"): Under EO 12333, U.S. intelligence agencies (such as the U.S. National Security Agency) may conduct surveillance outside the United States. Specifically, U.S. intelligence agencies are authorized to collect foreign "signals intelligence," i.e., information derived from communications and other data transmitted or accessible by radio, wire, and other electromagnetic means.

**Risk level for the persons concerned:** Microsoft Deutschland GmbH is a European subsidiary of Microsoft from the USA. Access from the USA can therefore not be ruled out. The contractor only processes the following data from [COMPANY]:

* + Name (first name, surname)
	+ Telephone number
	+ e-mail address
	+ Profile picture

Typically, no information is processed where there is a suspicion that knowledge of the US security authorities poses particular risks for users.

**Basis for data transfer to the USA:** EU standard contractual clauses from Microsoft:<https://learn.microsoft.com/de-de/compliance/regulatory/offering-eu-model-clauses> or Transatlantic Privacy Framework

**Technical security measures:** The "supplementary measures" of Elara Digital GmbH are attached to this contract as Annex 2a.

**Organizational measures:** The "supplementary measures" of Elara Digital GmbH are attached to this contract as Annex 2a.

**Appendix 2a**

**Technical safety precautions:**

* Type of data encryption used:
	+ Several strong encryption protocols and technologies are used to ensure the security and confidentiality of data. This includes the use of technologies such as Transport Layer Security/Secure Sockets Layer (TLS/SSL) for secure data transmissions, Internet Protocol Security (IPSec) for secure internet communication and Advanced Encryption Standard (AES) for robust data encryption. These measures offer a high level of protection against unauthorized access and data leaks. For more information visit <https://learn.microsoft.com/de-de/purview/encryption>.
* Systems and processes for monitoring and incident response:
	+ Advanced monitoring systems and incident response processes are implemented to proactively monitor and respond to security incidents. These systems continuously monitor the IT infrastructure, detect anomalies and unusual activities and enable a rapid response to security incidents. Detailed information can be found at <https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure-monitoring>.

**Organizational measures:**

* Data center locations and their data protection standards:
	+ The locations of the data centers are strategically chosen in Germany, specifically in Frankfurt, to comply with the strictest data protection standards and laws. This ensures that data is stored and processed within the EU, which meets the requirements of the GDPR. Further details can be found at <https://azure.microsoft.com/de-de/explore/global-infrastructure/data-residency/#overview>.
* Type of contractual agreements with subcontractors regarding data protection:
	+ Ensuring that all subcontractors adhere to strict data protection agreements that comply with GDPR regulations. This includes contractual assurances of compliance with data protection standards, regular reviews and audits and the obligation to report data breaches immediately. You can find additional information at [https://learn.microsoft.com/de-de/compliance/regulatory/gdpr?view=o365-worldwide verfügbar](https://learn.microsoft.com/de-de/compliance/regulatory/gdpr?view=o365-worldwide).

**Appendix 3**

**Data Protection Officer**

Dominik Adamowski

Brunsbütteler Damm 356

13591 Berlin

Phone: +49 176 4733 8214

dominik@getelara.de