Agreement on commissioned processing according to Art. 28 DSGVO

- as the responsible party, hereinafter referred to as the Client -

and
Elara Digital GmbH, Chausseestraße 103, 10115 Berlin
- as processor, hereinafter referred to as contractor -.

Preamble

Aim of this agreement

The Customer 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 the "Agreement") sets out in concrete terms the obligations of the contracting parties under data protection law, which arise in particular from Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals about the processing of personal data, on 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 commissioned by it and approved in advance by the Client (subcontractors) process the Client's personal data or may come into contact with such data. Insofar as the term "data" is used in the following, this shall, in case of doubt, mean the personal data of the Client.

§ 1

Subject matter and duration of the agreement

(regarding Art. 28 Par. 3 DSGVO)

The subject matter and duration of the order shall be determined in full by the information provided in the respective contractual relationship (Contract for the use of the Elara software). The Contractor shall process personal data for the Client within the meaning of Art. 4 No. 2 and Art. 28 DSGVO based on this order.

§ 2

Scope, nature, and purpose of commissioned processing, type of data, group of data subjects

(regarding Art. 28 (3) DSGVO)

2.1 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 offered software by the Client and its employees.

2.2 Type of personal data (Art. 4 No.1 DSGVO):

Customer data

- Name (first name, last name)
- Telephone number
- E-mail address
- Profile picture
- Comments

Employee data of the customer

- Name (first name, last name)
- Phone number
- E-mail address
- Profile picture
- Comments

2.3 Categories of persons concerned:

- Client
- Customer employee

§ 3

Instructions and powers to issue instructions

(regarding Art. 28 Par. 3 lit. a, 29 DSGVO)

3.1 The Contractor shall process the Client Data only within the scope of the commission and exclusively on behalf of and by the instructions of the Client within the meaning of Art. 28 DSGVO (commissioned processing), this shall apply in particular with regard to the transfer of personal data to a third country or to an international organization. In this respect, the Principal shall have the sole right to issue instructions regarding the type, scope and method of the processing activities (hereinafter also referred to as the "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.

3.2 Instructions shall generally be issued by the Customer in writing; instructions issued verbally shall be confirmed by the Customer in text form. If the Contractor is of the opinion that an instruction of the Customer violates data protection provisions, it shall notify the Customer thereof without undue delay. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer.

§ 4

Technical and organizational measures,

Data protection and data security concept

(regarding Art. 28 Par. 3 lit. c DSGVO)

4.1 The Contractor is obliged 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. The Customer shall demonstrate compliance with the obligations set forth in this Agreement by appropriate means.

4.2 Furthermore, the Contractor shall oblige all persons entrusted by it with the processing and fulfillment of this Agreement (hereinafter referred to as "Employees") in writing to maintain confidentiality (Art. 28 (3) lit. b DSGVO) and ensure compliance with this obligation with due care. Upon request of the Customer, the Contractor shall provide the Customer with evidence of the obligation of the Employees in writing or in electronic form.

4.3 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 DSGVO, in particular the measures listed in Annex 1 to this Agreement, and to maintain them for the duration of the processing of the Client Data.

4.4 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. The Contractor shall inform the Customer in writing without undue delay if it has reason to believe that the measures pursuant to Annex 1 are no longer sufficient and shall consult with the Customer regarding further technical and organizational measures.

4.5 At the request of the Customer, the Contractor shall provide the Customer with suitable evidence of compliance with the technical and organizational measures specified in Annex 1.

§ 5

Obligations of the contractor

(regarding Art. 28 Par. 3 lit. b, e, f DSGVO)

5.1 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 the Contractor within the scope of the order or by third parties, the Contractor shall inform the Client in electronic form without undue delay, but no later than within 48 hours after becoming aware of the same. The time of receipt by the Client shall be decisive for compliance with the

time limit. The same shall apply to audits of the Contractor by the data protection supervisory authority. The notifications shall in each case contain at least the information specified in Art. 33(3) of the GDPR.

5.2 In the aforementioned cases, the Contractor shall support the Client in fulfilling its clarification, remedial and information measures in this regard to the extent reasonable. In particular, the Contractor shall immediately implement the necessary measures to secure the data and to mitigate possible adverse consequences of the data subjects, inform the Customer thereof and request the Customer for further instructions.

The client is responsible for protecting the rights of the data subject. Against this background, the Contractor is nevertheless obliged, depending on the type of processing, to support the Client with appropriate technical and organizational measures in its, the Client's, obligation to respond to requests to exercise the rights of the data subject referred to in Chapter III of the GDPR, i.e. in responding to requests from data subjects with regard to the Client's information obligations towards the data subjects, their right of access, their right to rectification, erasure, restriction of processing, data portability and the client's related notification obligations, the right to object or to automated decision-making, including profiling, if the data subject asserts corresponding rights. If the data subject contacts the contractor directly to assert a right, the contractor shall forward the data subject's requests to the client without delay.

5.3 The Contractor undertakes to provide the Customer, upon the latter's verbal or written request and within a reasonable period of time, with all information and evidence required to carry out a control pursuant to § 7 of this Agreement. Furthermore, the Contractor shall provide the Customer, at the latter's request, with a comprehensive and up-to-date data protection and security concept for the commissioned processing as well as on persons authorized to access the data.

5.4 At the request of the Customer, the Contractor shall be obliged to keep a register of all categories of processing activities carried out on behalf of the Customer pursuant to Art. 30(2) of the GDPR. The directory shall be made available to the Customer upon request.

5.5 The Contractor is 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.

5.6 The Contractor confirms that - insofar as there is a legal obligation to do so - it has appointed a data protection officer. The complete contact details of the data protection officer shall be provided to the Customer in text form upon conclusion of the contract. A change in the person of the company data protection officer/contact person for data protection shall be notified to the Customer in writing without delay.

5.7 Should the Customer Data at the Contractor be endangered by seizure or attachment, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Customer 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.

5.8 The Contractor shall be entitled to reasonable compensation for support services under this provision.

5.9 All data of the client are stored in a suitable form so that they can be clearly identified and mixing with other clients is excluded.

§ 6

Subcontracting relationships

(regarding Art. 28 Para. 2, Para. 3 lit. d, Para. 4 DSGVO)

6.1 Within the scope of its contractual obligations, the Contractor is not authorized to establish subcontracting relationships with subcontractors ("Subcontractor Relationship"). Exceptions are only permitted after prior express written consent of the Customer in individual cases; this shall be deemed granted for the

subcontractors named in Annex 2. In any case, the Contractor shall ensure that the provisions agreed in this Agreement shall also apply vis-à-vis the subcontractors engaged by it, whereby the Customer shall be granted all rights of control vis-à-vis the subcontractor pursuant to this Agreement. Subcontractor relationships with third parties outside the European Economic Area are not permitted.

6.2 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, telecommunications services without any specific reference to services provided by the Contractor to the Customer 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.

§ 7

Control Rights of the Customer, Obligations of the Contractor to Tolerate and Cooperate

(regarding Art. 28 Par. 3 lit. h DSGVO)

7.1 The Customer shall be entitled to satisfy itself prior to the commencement of data processing and thereafter on a regular basis of compliance with all data protection requirements and agreements made, in particular the technical and organizational measures taken by the Contractor (see Annex 1). The Customer may also have this control carried out by a third party. The Contractor may provide evidence in individual cases by complying with approved rules of conduct pursuant to Art. 40, 41 of the GDPR or by means of a suitable and approved certification procedure pursuant to Art. 42 of the GDPR.

7.2 The Customer 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.

7.3 The Customer shall document the inspection result and notify the Contractor thereof. In the event of errors or irregularities which the Customer discovers, in particular during the inspection of order results, the Customer shall inform the Contractor without delay. If facts are found during the inspection, the future avoidance of which requires changes to the ordered procedure, the Customer 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 termination of the order

(regarding Art. 28 Para. 3 lit. g DSGVO)

8.1 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 which serves as proof of the proper processing of the Client Data in accordance with the order. Such documentation shall be handed over by the Contractor to the Client upon request.

8.2 The Contractor shall confirm the deletion to the Client in writing. The Client has the right to control the complete and contractually compliant return or deletion of the data at the Contractor in an appropriate manner.

8.3 The Contractor shall be entitled to remuneration for services under this provision.

§ 9
Place of processing
(regarding Art. 28 Par. 3 lit. a DSGVO)

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 contracting state of the Agreement on the European Economic Area, provided that it 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. He is free in his decision in this respect. The Contractor shall ensure that, in the event of transfer to a third country, the specific legal requirements are met (Art. 44 et seq. DSGVO).

§ 10

Termination of contract

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

§ 11

Liability

The liability of the parties shall be governed by Art. 82 DSGVO. Any liability of the Contractor towards the Client due to breach of obligations under this Agreement or the Main Agreement shall remain unaffected.

§ 12

Final provisions

12.1 Amendments and supplements to this agreement must be made in writing. This shall also apply to any deviation from this written form requirement. Amendments and supplements require express reference to the fact that they are an amendment or supplement to these terms and conditions.

12.2 Should any provision of this agreement be invalid, this shall not affect the validity of the remaining provisions. The parties undertake to agree on a valid provision that comes as close as possible to the invalid provision in place of the invalid provision.

12.3 German law shall apply. The place of jurisdiction shall be determined by the provisions in the main contract.

12.4 In the event of contradictions or regulatory conflicts between this Data Processing Agreement (DPA) and the main contract, the main contract shall take precedence, unless and insofar as mandatory data protection provisions require this DPA to take precedence.

Attachment 1
Data protection and data security concept

A. Confidentiality (Art. 32 para. lit. b DSGVO)

1. Access control

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

a. Measures at company headquarters

Alarm system with connection to security service or police	Written regulations on access authorization
Automatic access control system	Manual closing system
Chip cards / transponder systems	Security locks
Biometric access barriers	Reception / Receptionist / Gatekeeper
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 confidentiality obligation	Visitors accompanied by staff for the entire duration of their visit
Care in the selection of external service providers who are granted access to the building (security guards, cleaning services, craftsmen, ...)	All external service providers (security personnel, cleaning services, tradesmen, ...) must sign a confidentiality agreement before entering the building for the first time
Written regulation for the selection and review of external service providers	Other measures:

b. Measures regarding server rooms

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

2. Access control

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

Written regulations on the granting of user accounts in place	Logging of user account allocation and revocation
Granting of user accounts only by administrators	Personalized user accounts only
Login with biometric data	Login with username + password
Password security policy in place (minimum password length and complexity)	Compliance with password security policy is technically enforced
Regular password change required	Access blocking in case of 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 developed

Anti-virus software for server	Anti-virus software for clients
Anti-virus software for mobile devices	Firewall
Any anti-virus software and firewall used is regularly updated	Intrusion Detection Systeme
Mobile Device Management	Mobile Device Policy
Housing lock	Use VPN for remote access
Encryption of notebooks / tablets *Bitlocker, FileVault.*	Encryption of data carriers *Bitlocker, FileVault.*

3. Access control

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

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

4. Separation control

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

Separation of productive and test environment	Separation of data from different controllers
Physical separation	Logical separation
Separation via authorization concept	*Other measures:*

5. Pseudonymization (Art. 32 para. 1 lit. a DSGVO; Art. 25 para. 1 DSGVO)

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

Pseudonymization of data is possible if required	Personal data is pseudonymized as soon as possible
Separation of assignment data to remove pseudonymization in separate and secured system	Personal data is made anonymous (reassignment to individuals is impossible no matter how much effort is required)
Cancellation of pseudonymization only possible if there is a legal basis and only for individual employees who have received special training in data protection law	Other measures:
Employees possible who have been specially trained in data protection law	

B. Integrity (Art. 32 para. lit. b DSGVO)

1. Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and determine to which entities personal data is 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) via mail, messenger or similar means The physical dispatch of personal data is carried out in compliance with suitable security measures: **Postal dispatch:** use of registered or insured mail for confidential or particularly sensitive data. **Courier services:** Commissioning of certified logistics service providers who comply with data protection and security requirements. **Transport encryption:** Strong encryption is used for electronic data carriers (e.g. USB sticks, hard drives) to prevent unauthorized access in the event of loss. **Documentation and tracking:** Dispatch of sensitive data is made traceable by confirmations of receipt or tracking mechanisms. **Access restriction:** Only authorized persons may send or receive physical data carriers.	Careful selection of transport personnel and vehicles
Use of safe transport containers	Documentation of data recipients as well as the duration of the planned transfer or the agreed deletion periods
Use of VPN for remote access	Disclosure of data only in pseudonymized form (for further details, see “Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)”)
Logging of regular retrieval and transmission processes	Logging every time data is retrieved
Locking external interfaces (e.g. USB)	Remote maintenance of systems in which personal data of the controller are stored
Privacy vault available	Clean-Desk-Policy
Shredder	Guideline for the deletion and destruction of data carriers
External document shredder Provider: Shred-IT	

2. Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed.

a) The Contractor shall process personal data of the Customer predominantly on the IT systems of the Customer. For these processing operations, no input control information is required from the Contractor. The following technical and organizational measures of the Customer shall apply with regard to input control, for the implementation and maintenance of which the Customer shall be responsible:

- The entry, modification and deletion of personal data shall be tracked by audit-proof logging in the respective applications.

- Detailed authorization concepts for the applications are implemented in the system and 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.

b) If, in individual cases, personal data of the Customer is processed on the IT systems of the Contractor, e.g. by means of transmitted screenshots of error messages or test data sets or similar, this shall be done exclusively for analysis purposes. This data is not transmitted back to the client in modified form for further use, but is deleted after the analysis has been completed at the contractor's premises. Therefore, no separate measures for input control are 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.

C. Availability and resilience of systems and services (Art. 32 para. lit. b, c DSGVO)

1. Availability control

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

a. General measures

Use of a spam filter	Written back-up and recovery concept
Automatic regular data backup	Appropriately frequent backup of data
Storing the backup media in a safe place	Retention period for back-ups 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	Other measures:

b. 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 case 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)	Other measures:

2. Rapid recoverability (Art. 32(1)(c) GDPR)

Measures to ensure that in the event of accidental destruction or loss of data, it can be recovered quickly.

Regular tests for data recovery	Logging the results of the data recovery tests
Other measures:	

D.Procedures for periodic review, assessment and evaluation of the effectiveness of the TOMs to ensure the security of processing (Art. 32 (lit.) d GDPR)

1. Data protection management (Art. 25 (1) GDPR)

Measures to ensure that all data protection requirements are complied with at all times.

Data protection management software solutions in use	Written data protection and data security concept available
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, adjustment of the protective measures takes place
Documentation of the verification of the effectiveness of the protective measures	Certification available
Existence of a processing directory in accordance with Art. 30 (2) DSGVO - Currently still in process	Periodic review and updating of the processing directory. -
Regular training of all employees (data protection as well as data security)	All employees are bound to confidentiality/data secrecy or are subject to a legal duty of confidentiality
If there is a corresponding legal obligation, the data protection impact assessment is carried out in accordance with Art. 35 DSGVO	Other measures:

2. Incident-Response-Management

Measures to ensure rapid and appropriate response to security breaches.

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

3. Privacy-friendly default settings (Art. 25 (2) GDPR)

Measures to ensure that the principles of privacy by design and privacy by default are observed.

No more personal data is collected than necessary for the respective purpose	Simple exercise of data subject rights possible
Automatic deletion of data after expiry ensured	Other measures:

4. 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 regulation on what is to be observed when selecting subcontractors
Documentation of the selection process	Authority to issue directives is clearly defined
Conclusion of the necessary contracts (order processing contract or standard contractual clauses) is ensured by appropriate guidelines	Order processing contracts comply with the requirements of Art. 28 DSGVO
Agreement on on-site inspections at the subcontractor's premises	Ongoing, regular review of the sub-service provider and its level of protection

The use of further service providers by the subcontractor is prevented	The subcontractor may in turn use other service providers
All requirements from the order processing contract with the controller are also contractually agreed with the sub-service provider	Other measures:

Attachment 2
List of subcontractors

Subcontractor	Address / Country	Service
Microsoft	Unter den Linden 17, 10117 Berlin	Server-Hosting, Azure-Blob Storage
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Server-Hosting

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

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.

Attachment 2a

Technical security 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 communications and Advanced Encryption Standard (AES) for robust encryption of data. 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. Additional information is available at https://learn.microsoft.com/de-de/compliance/regulatory/gdpr?view=o365-worldwide

Attachment 3
Data Protection Officer

DataCo GmbH
Sandstraße 33
80335 München
datenschutz@dataguard.de