Deutscher Akademischer Austauschdienst
German Academic Exchange Service

Data Processing Agreement

The
German Academic Exchange Service (DAAD), Kennedyallee 50, 53175 Bonn

- Data Controller -

and
the company [**name and contact details of the data processor(s)**]

- Data Processor -

enter into this agreement, including its subsequent binding annexes, to fulfil the requirements of Article 28 of the General Data Protection Regulation (GDPR)[1] , whereby the subject matter and purpose of the processing are derived from the written main agreement

Framework Agreement for the delivery of English language courses in the United Kingdom (UK) for teaching staff at German higher education institutions, Contract No. 100/2026 dated [**date of award**].

Annex 1 Description of the processing

Annex 2 Contact person and instructions from the data controller

Annex 3 Technical and organisational measures in accordance with Article 32 of the GDPR

Appendix 4 Sub-processors

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

1. Definitions, priority clause

1.1. The definitions set out in the GDPR apply.

1.2. In the event of any conflict between this contract and any other contracts between the parties, the provisions of this contract shall prevail.

2. Rights and obligations of the controller

The controller shall be responsible, in particular, for the lawfulness of the processing in accordance with Article 6(1) of the GDPR or other relevant legal bases, compliance with the data protection law of the Member States applicable to and binding upon the controller, and the safeguarding of the rights of data subjects under Articles 7, 12 to 22 of the GDPR.

3. Processing in accordance with instructions and the duty to object

3.1. The contact persons listed in **Annex 2** are responsible for instructions from the controller to the processor[2] (Article 29 in conjunction with Article 28(3)(a) of the GDPR). The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of those legal requirements prior to processing, unless such notification is prohibited by the relevant law on grounds of an important public interest. Within the scope of an instruction, the processor may retain a degree of discretion as to which appropriate technical and organisational measures are used to implement the instruction. Furthermore, processing by the processor shall be carried out in accordance with any instructions set out in **Annex 2**.

Editing note: *Please select at least one of the two options. The option not selected may be removed.*

[2] This model contract generally applies only to processors established in an EEA Member State or in a third country for which an adequacy decision has been adopted by the European Commission pursuant to Article 45 of the GDPR. Otherwise, the European Commission's standard data protection clauses pursuant to Article 46(2) of the GDPR may be used.

3.2. Instructions are generally issued by the controller in writing (e.g. by email). Insofar as an instruction is, exceptionally, given orally, this shall be

☒ data processor

☐ controller

confirmed in writing (e.g. by email). The processor shall ensure that all instructions issued by the controller are communicated to its relevant employees (e.g. by centrally filing all instructions).

3.3. The processor shall immediately inform the controller if, in its opinion, compliance with an instruction issued by the controller would contravene the GDPR or any other data protection regulation (duty to object). In such a case, it may suspend implementation of the instruction until the controller indicates whether it intends to maintain, amend or revoke the instruction.

4. Confidentiality

The processor shall, for the performance of the contract, only employ persons whom it has bound to confidentiality or who are subject to an appropriate statutory duty of confidentiality. In this respect, the processor shall ensure that these persons only access personal data relating to the commissioned processing activity to the extent necessary ('need to know'). Insofar as the controller is subject to statutory confidentiality obligations, the processor shall oblige the employees engaged in the performance of the contract, as well as any sub-processors, to maintain confidentiality, taking into account relevant law, in particular the relevant professional code of conduct.

5. Technical and organisational measures in accordance with Article 32 of the GDPR

5.1. The processor shall implement all necessary technical and organisational measures in accordance with Article 32 of the GDPR, which shall include at least the measures specified in **Annex 3**.

5.2. Technical and organisational measures are subject to technical progress and further development. During the term of this contract, the processor shall continuously adapt these measures to the requirements of this contract and further develop them in line with technical progress. The adequacy of the measures shall be reviewed regularly by the processor. The level of security of the technical and organisational measures set out in **Annex 3** must not be reduced without the written consent of the controller. Written consent may also be provided in electronic format.

5.3. The processor undertakes to document in writing any changes to the technical and organisational measures that have a significant impact on the guaranteed level of security as an addendum to **Annex 3**, which may also be in electronic format, and to notify the controller thereof.

6. Use of sub-processors

6.1. The Data Processor may engage sub-processors provided that they offer sufficient guarantees with regard to expertise, reliability and resources. Any sub-processors engaged at the time of conclusion of the contract are listed in **Annex 4** to this contract

The processor shall inform the controller in writing, which may also be in electronic format, of any intended change regarding the engagement or replacement of sub-processors and shall provide the necessary information to exercise the right to object within the framework of the aforementioned, updated list. The controller may object to such changes within a period of 4 weeks. During this period, the sub-processor may not be engaged. If the controller objects to the engagement or replacement of a sub-processor, the controller and the processor shall consult with each other within a period of 4 weeks to determine to what extent the involvement of the sub-processor can be restricted or excluded in accordance with the controller's instructions, or whether the contract – taking into account the relevant notice periods – is to be terminated.

6.2. Where the processor engages the services of a sub-processor to carry out specific processing activities on behalf of the controller, that sub-processor shall be bound by a contract, which shall be in writing, including in electronic form, or by any other legal

instrument under Union law or the law of the Member State concerned, essentially the same data protection obligations as those laid down in this contract, in particular providing sufficient guarantees that appropriate technical and organisational measures are implemented so that the processing is carried out in accordance with the requirements of the GDPR. Where a sub-processor breaches its resulting obligations, the processor shall inform the controller accordingly. The processor shall ensure that each sub-processor fulfils the processor's obligations under this contract and the GDPR. Furthermore, the controller must be entitled to carry out audits and inspections, including on-site, at the premises of such a sub-processor or to have them carried out by third parties appointed by the controller. If the sub-processor fails to fulfil its data protection obligations, the processor shall be liable to the controller for the sub-processor's compliance with its obligations.

6.3. If the processor uses the services of a sub-processor, it shall agree with the latter on a third-party beneficiary clause, whereby the controller – in the event that the processor ceases to exist de facto or de jure or becomes insolvent – shall assume the rights and obligations of the defunct data processor under its data processing agreement with the sub-processor and shall have the option of terminating that contractual relationship and instructing the sub-processor to erase or return the personal data.

7. Transfers to third countries

7.1. A transfer of personal data to a third country or an international organisation shall only take place on the documented instructions of the controller and in accordance with Chapter V of the GDPR.

7.2. In the case referred to in paragraph 1, the processor may enter into the EU Commission's Standard Data Protection Clauses (the 'Processor to Processor' module) with any sub-processor in accordance with Article 46(2) of the GDPR.

8. Obligations to cooperate and assist

The processor shall, in view of the nature of the processing , assist the controller with appropriate technical and organisational measures in fulfilling its obligation to respond to requests for the exercise of the data subject's rights set out in Chapter III of the GDPR and shall, in this respect, take into account the controller's instructions. Where data subjects contact the processor to exercise their rights, the processor shall inform the controller without delay. In this regard, the contact persons listed in **Annex 2** are responsible. The processor shall only respond to a data subject's request after authorisation by the controller.

9. Support for the controller's fulfilment of its obligations

9.1. The processor shall assist the controller, taking into account the nature of the processing and the information available to it, in complying with the obligations set out in Articles 32 to 36 of the GDPR (ensuring the security of processing; notifying supervisory authorities of personal data breaches; notifying the data subject affected by a personal data breach; data protection impact assessment; prior consultation) and shall, in this regard, ensure the technical and organisational measures described in **Annex 3**.

9.2. If the processor becomes aware of a personal data breach, it shall notify the controller without undue delay in writing, taking into account the requirements set out in Article 33(3) and (4) of the GDPR. In this regard, the contact persons listed in **Annex 2** are responsible.

10. Deletion and return of personal data

10.1. Unless precluded by statutory or other retention obligations, the processor shall – subject to any other instructions from the controller pursuant to clause 3 – upon termination of the contract, delete the personal data used

☒ and any existing copies in accordance with data protection regulations following **written** notification to the controller and the expiry of a period of 4 weeks from receipt of such notification.

10.2. The processor shall confirm to the controller in writing any such deletion. If statutory or other retention obligations prevent deletion or handover, the processor shall inform the controller accordingly in writing.

10.3 Until the data is deleted or returned, the processor shall continue to ensure compliance with this contract.

11. Record of obligations and assistance with audits

11.1. The parties must be able to demonstrate compliance with this Agreement.

11.2. The Data Processor shall, upon request, provide the Data Controller with all necessary information and documents to demonstrate compliance with the obligations set out in Article 28 of the GDPR and in this Agreement, including any contracts with sub-processors. To the extent necessary to protect trade secrets or other confidential information, including personal data, the processor may redact the text of any contracts before providing a copy.

11.3 It shall permit audits – including inspections at the premises or physical facilities of the processor, where appropriate with reasonable notice – to be carried out by the controller or another auditor appointed by the controller, and shall assist in their conduct. The determination of the manner in which the audit is to be conducted (e.g. remotely or on-site, via questionnaire or in a face-to-face interview) is subject to the data controller's unrestricted discretion. The data controller may, at its discretion, also base its audit on an audit carried out on behalf of the data processor, as well as on relevant certifications held by the data processor.

11.4. The processor shall respond to contract-related enquiries from the controller promptly and in an appropriate manner.

11.5. The parties shall, upon request, provide the competent supervisory authority with the information referred to in clauses 11.1–11.3, including the results of any audits.

12. Miscellaneous provisions

12.1. Should the fulfilment of the subject matter of the contract in accordance with **Annex 1** by the processor be jeopardised by attachment or seizure, by insolvency or composition proceedings, or by other events or measures taken by third parties, the processor shall inform the controller without delay. The Data Processor shall immediately inform all parties involved in this context that the authority to dispose of the data lies exclusively with the Data Controller.

12.2. The Data Processor shall inform the Data Controller without delay if it is unable to fulfil the obligations under this contract. Insofar as the Data Processor fails to fulfil obligations under this contract, the Data Controller may instruct the Data Processor to suspend processing until the Data Processor's contractual obligations are guaranteed. If the processor fails to ensure compliance with its contractual obligations or with the GDPR within a reasonable period (at the latest within one month), the controller may terminate the contract with immediate effect. The controller shall also have the right to terminate the contract without notice in the event of a serious breach by the processor of this contract or of obligations under the GDPR. The same shall apply if the processor fails to comply with a court order or a decision by the competent supervisory authority that is binding on it.

12.3. Should individual provisions of this contract be invalid, this shall not affect the validity of the remainder of the contract.

12.4. Any amendment to this Agreement, including its termination and this clause, must be in writing, which may also be in electronic form.

[**Place**], [**Date**] Bonn,

- Data *processor* -	- DAAD as data *controller* -

Annex 1 to the Data Processing Agreement: Description of the processing

Subject matter and purpose of the processing

The subject matter and purpose of the processing are set out in the written main contract

Framework Agreement on the delivery of English language courses in the United Kingdom (UK) for teaching staff at German higher education institutions,
Contract No. 100/2026 dated [date of award]

Duration of processing

The duration of the processing is set out in the written main contract.

Nature of the processing

The data will be processed by

☒ collection

☒ recording

☒ recording

☒ organisation

☒ sorting

☒ storage,

❒ archiving,

☒ adaptation or modification

☒ retrieval

☒ retrieval

☒ the use

☒ disclosure through transmission

☒ dissemination or any other form of provision

☒ the comparison or linking

❒ restriction

☒ erasure or destruction

❒ other types of processing:

Categories of personal data

Categories of personal data subject to processing:

☒ Address details (postal address)

☒ Billing and payment data

☒ Names

☐ User IDs

☒ Age

☐ Passwords

☐ Working time data

☐ Personal master data

☒ Audio data

☒ Planning and control data

☐ Bank details

☐ Personnel and identification numbers

☒ Applicant data

☒ Travel booking and expense claim data

☒ Image data

☒ Email addresses

☐ Telecommunications billing data

☐ Telecommunications connection data

☒ Telephone numbers

☐ Hobbies

☐ Contract details

☐ Credit card details

☐ Customer behaviour data

☐ Communication data

☐ Customer history

☐ Payroll data

☐ Employee appraisals

☐ Employee qualifications and characteristics

☒ Video data

☐ Access data

☐ Other categories of personal data:

Categories of sensitive personal data

[3]***Processing note:*** Sensitive data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or which contains genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning a person's health, sex life or sexual orientation, or data relating to criminal convictions and offences.

Categories of sensitive personal data subject to processing (if any):

☐ Health data

☐ Religious affiliation

☐ Trade union membership

☐ Political opinions

☐ Other categories of sensitive personal data:

Restrictions or safeguards applied that take full account of the nature of the sensitive personal data and the associated risks:

☐ Strict purpose limitation

☐ Access restrictions (including access only for staff who have undergone specific training)

☐ Records of access to the data

☐ Restrictions on onward transfers

☐ additional security measures **[…] Please complete!**

☐ Other restrictions or safeguards **[…] Please complete!**

[3] The use of the term 'racial origin' corresponds to the wording of the GDPR. The use of this term in this Regulation does not imply that the Union endorses theories seeking to establish the existence of different human races (Recital 51(2) of the GDPR).

Categories of data subjects

In the course of performing the contract, the data processor processes personal data relating to the following categories of data subjects:

☒ Employees

☒ Trainees and interns

☐ Job applicants

☐ Former employees

☐ Freelancers

☒ Club members

☒ Beneficiaries

☐ Alumni

☐ Relatives of employees

☐ Customers

☒ Prospective candidates

☐ Suppliers and service providers

☒ Tenants

☒ Business partners

☐ Consultants

☐ Visitors

☐ Press representatives

☐ Subscribers

☐ Sales representatives

☐ Contact persons

☐ Other categories of data subjects:

Annex 2 of the AV contract: Contact persons and instructions from the controller

Processing note: *Contact details for the relevant contact persons, including deputies, should be added. In this regard, it is recommended that contact channels be set up that are role-based rather than person-specific (e.g. ds-verletzung@xyz.de, ds-betroffenenanfrage@xyz.de, ds-weisung@xyz.de).*

Reason	**Role/function of the contact person at the controller**	**Role/function of the contact person at the data processor**
Instructions	info@daad-akademie.de	
Data subject requests	datenschutz@daad.de	
Data breaches at the data processor	datenschutz@daad.de	
Inspections/Audits	datenschutz@daad.de	

Processing note: *At this point, instructions from the controller may optionally be incorporated into this contract. In this respect, the processor may retain a degree of discretion as to which appropriate technical and organisational measures are used to implement the instructions.*

Short description of the instruction	**Description of the instruction**

Annex 3 of the Data Processing Agreement: Technical and organisational measures in accordance with Article 32 of the GDPR

Editing note: *This Annex 3 is to be completed by the data processor. It specifies the technical and organisational measures taken by the data processor.*

Taking into account the

- state of the art,
- the implementation costs,
- the nature, scope, context,
- the purposes of the processing,
- the sensitivity of the personal data being processed, in particular with regard to special categories of personal data (see Article 9(1) of the GDPR), as well as
- the varying likelihood and severity of the risk to the rights and freedoms of natural persons

the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

When assessing the appropriate level of protection, particular account must be taken of the risks associated with the processing, in particular those arising from – whether accidental or unlawful – destruction, loss, alteration or unauthorised disclosure of, or unauthorised access to, personal data that has been transmitted, stored or otherwise processed.

The processor shall take the following measures:

1. Measures to ensure confidentiality

It must be ensured that personal data is processed exclusively by authorised persons.

1.1. Access control

Unauthorised persons must be denied access to data processing facilities used to process or utilise personal data.

☐ Access control system, ID card reader (magnetic/chip card)

☐ Door security measures (electric door openers, combination locks, etc.)

☐ Security doors / windows

☐ Bars on windows/doors

- ☐ Fencing
- ☐ Key management/documentation of key allocation
- ☐ Site security, gatekeepers
- ☐ Alarm system
- ☐ CCTV
- ☐ Special security measures for the server room
- ☐ Special security measures for the storage of backups and/or other data storage media
- ☐ Irreversible destruction of data storage media
- ☐ Staff and access cards
- ☐ Restricted areas
- ☐ Visitor policy (e.g. collection at reception, recording of visit times, visitor passes, escorting visitors to the exit after their visit)
- ☐ Other/Specification of the above measures: [**Please elaborate**]

1.2. Access control

It must be ensured that data processing systems cannot be used by unauthorised persons.

- ☐ Personal and individual user log-in when logging into the system or company network
- ☐ Authorisation process for access rights
- ☐ Restriction of authorised users
- ☐ Single sign-on
- ☐ Two-factor authentication
- ☐ Biometric scan (fingerprint, iris, face)?
- ☐ BIOS passwords
- ☐ Password policy (specification of password parameters regarding complexity and update interval)
- ☐ Automatic blocking of access for a specific period following repeated incorrect entry of login details?

- ☐ Electronic documentation of passwords and protection of this documentation against unauthorised access
- ☐ Personalised smart cards, tokens, PIN/TAN, etc.
- ☐ Logging of access
- ☐ Additional system log-in for specific applications
- ☐ Automatic locking of clients after a certain period of inactivity (including password-protected screensavers or automatic sleep mode)
- ☐ Firewall
- ☐ System-specific protection against attacks / intrusion detection / intrusion prevention
- ☐ Other/Specification of the above measures: [**Please elaborate**]

1.3. Access control

It must be ensured that persons authorised to use a data processing system can access only the data covered by their access authorisation, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage.

- ☐ Management and documentation of granular permissions
- ☐ Analysis/logging of data processing
- ☐ Authorisation process for permissions
- ☐ Approval procedures
- ☐ Profiles/roles
- ☐ Regular checks of access rights in accordance with the 'need-to-know' principle
- ☐ Encryption of CD/DVD-ROMs, external hard drives and/or laptops (e.g. via the operating system)
- ☐ Measures to prevent unauthorised transfer of data to external storage media (e.g. copy protection, blocking of USB ports, 'Data Loss Prevention (DLP) system')
- ☐ 'Mobile Device Management system'
- ☐ Dual-control principle
- ☐ Segregation of duties

☐ Professional destruction of files and data carriers in accordance with DIN 66399

☐ Irreversible erasure of data storage media

☐ Logging/documentation of erasure

☐ Privacy screens for mobile data processing systems

☐ Other/Specification of the above measures: [**Please specify**]

1.4. Separation control

It must be ensured that data collected for different purposes can be processed separately.

☐ Storage of data records in physically separate databases

☐ Separate systems

☐ Access permissions based on functional responsibility

☐ Separate data processing through differentiated access controls

☐ Multi-client capability of IT systems

☐ Use of test data

☐ Separation of development and production environments

☐ Other/Specification of the above measures: [**Please elaborate**]

2. Encryption measures

It must be ensured that access to plain text is only possible using a (secret) key.

☐ Encryption of mobile devices such as laptops, tablets and smartphones

☐ Encryption of mobile storage media (CD/DVD-ROM, USB sticks, external hard drives)

☐ Encryption of files

☐ Encryption of systems/equipment

☐ Encrypted storage of passwords

☐ Encryption of emails and email attachments

☐ Secure data transfer (e.g. SSL, FTPS, TLS)

☐ Secure Wi-Fi

☐ Other/Details of the above measures: [**Please specify**]

3. Pseudonymisation

Personal data shall be processed in such a way that the personal 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 technical and organisational measures ensuring that the personal data is not attributed to an identified or identifiable natural person.

Pseudonymisation is a technical and organisational measure and can be implemented by the processor as follows:

- ☐ separate storage of additional information for identification
- ☐ Use of (staff, customer or patient) identification numbers instead of names
- ☐ Encryption of additional identification information
- ☐ Management and documentation of differentiated access rights to additional identification information
- ☐ Authorisation process or approval procedures for permissions to process additional identification information
- ☐ Copy protection regarding supplementary identification information
- ☐ Dual-control principle for identification
- ☐ Other/Specification of the above measures: [**Please elaborate**]

4. Measures to ensure integrity

It must be ensured that personal data is processed correctly and free from manipulation.

- ☐ Access rights
- ☐ System-level logging
- ☐ Document Management System (DMS) with change history
- ☐ Security/logging software
- ☐ Functional responsibilities, organisationally defined responsibilities
- ☐ Dual control principle
- ☐ Tunnelled remote data connections (VPN = Virtual Private Network)
- ☐ “Data Loss Prevention (DLP) system”
- ☐ Electronic signature

☐ Logging of data transmission or data transfer

☐ Logging of read accesses

☐ Logging of copying, modification or deletion of data

☐ Other/Specification of the above measures: [**Please specify**]

5. Measures to ensure and restore availability

It must be ensured that personal data is protected against accidental destruction or loss.

☐ Security concept for software and IT applications

☐ Back-up procedures

☐ Storage process for backups (fireproof safe, separate fire compartment, etc.)

☐ Ensuring data storage within a secure network

☐ Installation of security updates as required

☐ Mirroring of hard drives

☐ Installation of an uninterruptible power supply (UPS)

☐ Suitable storage facilities for paper documents

☐ Fire and/or water protection for the server room

☐ Fire and/or water damage protection for the archive facilities

☐ Air-conditioned server room

☐ Virus protection

☐ Firewall

☐ Contingency plan

☐ Successful emergency drills

☐ Redundant, geographically separate data storage (offsite storage)

☐ Other/Specification of the above measures: [**Please elaborate**]

6. Measures to ensure resilience

It must be ensured that the data processing systems are sufficiently robust and resilient to cope with the most significant anticipated incidents without their functionality being impaired.

☐ Contingency plan for machine failure

☐ Redundant power supply

☐ Sufficient capacity of IT systems and equipment

☐ Logistically managed process to prevent peak loads

☐ Redundant systems/equipment

☐ Resilience and fault management

☐ Other/Specification of the above measures: [**Please elaborate**]

7. Effectiveness monitoring

It must be ensured that procedures are in place for the regular review, assessment and evaluation of the effectiveness of the technical and organisational measures.

☐ Procedures for regular checks/audits

☐ Concept for regular review, assessment and evaluation

☐ Reporting

☐ Penetration tests

☐ Disaster recovery testing

☐ Certification; if available, [**Please specify**]

☐ Other/Specification of the above measures: [**Please specify**]

8. Instruction control

It must be ensured that personal data is processed only in accordance with the instructions of the controller (including by a processor).

☐ Data processing agreement pursuant to Article 28(3) of the GDPR, setting out the rights and obligations of the processor and the controller

☐ Guidelines/specifications for defining data protection responsibilities/accountabilities

☐ Process for issuing and/or complying with instructions

☐ Designation of contact persons and/or responsible staff members

☐ Monitoring/review of order execution in accordance with instructions

☐ Training/induction of all employees with access rights at the data processor

☐ Independent audit of compliance with instructions

☐ Employees' obligation to maintain confidentiality

☐ Agreement on contractual penalties for breaches of instructions

☐ Appointment of a data protection officer in accordance with Article 37 et seq. of the GDPR

☐ Data Protection Manager/Coordinator

☐ Maintaining a record of processing activities in accordance with Article 30(2) of the GDPR

☐ Documentation and escalation process for personal data breaches

☐ Guidelines/requirements for ensuring technical and organisational measures for the security of processing

☐ Other/Specification of the above measures: [**Please elaborate**]

9. Support for the controller

The processor shall provide the necessary support to the controller in fulfilling its obligation

- *to respond to requests for the exercise of the data subject's rights as set out in Chapter III of the GDPR,*
- *in reporting data breaches to the competent supervisory authorities and data subjects,*
- *in carrying out a data protection impact assessment, including any necessary consultation with the competent supervisory authority, and*
- *in its duty to ensure the required data quality (factually correct and up to date).*

☐ Guidelines/specifications for defining data protection responsibilities/accountabilities

☐ Guidelines/requirements for ensuring technical and organisational measures for the security of processing

☐ Process for forwarding data subject requests

☐ Notification of the controller upon becoming aware of inaccurate or outdated personal data

☐ Other/Specification of the above measures: [**Please elaborate**]

Compliance with approved codes of conduct pursuant to Article 40 of the GDPR or an **approved certification procedure** pursuant to Article 42 of the GDPR as a factor in demonstrating compliance with the above requirements (1 to 8):

☐ [**Please elaborate**]

Existence of recognised certificates relating to the above requirements (e.g. ISO 27000 series):

☐ [**Please specify**]

Annex 4 of the Data Processing Agreement: Sub-processors

Instructions: *This Annex 4 is to be completed by the data processor.*

Name and address of the sub-processors	Subject matter, nature and duration of the sub-processing	Information required for the controller's decision on approval/objection, in particular a description of the evidence of appropriate technical and organisational measures (e.g. contract, documented policy)
