

Annex 1 to the Nexis 4 Platform Terms and Conditions

Data Processing Agreement pursuant to Art. 28 GDPR

Hereinafter, the Controller and Nexis shall each be referred to as a “**Party**” and collectively as the “**Parties**”. For the purposes of this Annex, the Controller within the meaning of this Annex is the Licensee.

Preamble

This Agreement governs the data protection obligations regarding the processing of personal data in the course of the services provided by Nexis under the NEXIS 4 Platform Terms and Conditions and in connection with the related offer (the “**Main Agreement**”).

Unless otherwise defined in this Agreement, the definitions set forth in the NEXIS 4 Platform Terms and Conditions shall apply accordingly.

1. Object and Term of the Order

- 1.1 Insofar as Nexis, in the course of performing the Main Agreement, obtains access to personal data that it processes on behalf of the Controller (“Subject Matter of the Processing”), the provisions of this Agreement shall apply. Details of the processing are set forth in Annex 1 (Description of the Processing), which forms an integral part of this Agreement.
- 1.2 The Subject Matter of the Processing shall be deemed an instruction within the meaning of Section 2.1.
- 1.3 Any change to the Subject Matter of the Processing shall require a corresponding written instruction from the Controller.

2. Processing Only on the Controller’s Instructions

- 2.1 Personal data may be processed solely on the Controller’s written instructions, in particular with regard to the transfer of personal data to a third country or to an international organization. Oral instructions shall be confirmed by the Controller without undue delay and without being requested to do so, in text form (e.g., by email).
- 2.2 If Nexis is obliged to process or transfer personal data without such instructions due to national law or Union law, Nexis shall notify the Controller in text form (by email) prior to commencing the relevant processing activity, unless such

notification is prohibited on the grounds of an important public interest or other compelling legal reasons.

- 2.3 Nexis shall inform the Controller without undue delay if it is of the opinion that an instruction from the Controller infringes applicable data protection provisions.

3. Confidentiality

Nexis shall require all persons engaged in the processing of personal data to commit themselves to confidentiality prior to commencing their activities, unless they are subject to an appropriate statutory duty of confidentiality.

4. Security of Processing

- 4.1 In accordance with Article 32 of the General Data Protection Regulation (Regulation (EU) 679/2016, "GDPR"), Nexis shall take the measures required to ensure an appropriate level of protection. The technical and organizational measures implemented by Nexis pursuant to Article 32 GDPR are set forth in Annex 2 (Technical and Organizational Measures), which forms an integral part of this Agreement.
- 4.2 Considering the nature of the processing and the information available to it, Nexis shall assist the Controller in complying with the obligations set out in Articles 32 to 36 GDPR.
- 4.3 Taking into account the nature of the processing, Nexis shall, through appropriate technical and organizational measures, assist the Controller in fulfilling its obligations to respond to requests for the exercise of the rights of data subjects as set forth in Chapter III of the GDPR.

5. Obligations to Provide Information and Rights of Inspection

- 5.1 The Controller shall have the right, at any time, to personally verify, or to have a representative appointed by them verify, compliance with the terms of this Agreement. Nexis shall grant the Controller or the Controller's appointed representative access to the essential premises related to the processing. Such inspections shall take place exclusively during Nexis's normal business hours and, unless a different arrangement is strictly required in an individual case, with prior notice of at least 14 working days. The Controller shall ensure that such inspections are conducted in a manner that interferes as little as possible with Nexis's business operations. Such an inspection shall generally take place no more than once per year. Each party shall bear its own costs for this annual inspection. Additional inspections shall only be conducted if there are specific indications of a breach of data protection obligations by Nexis. If, during such an

additional inspection, it is found that Nexis has not breached its data protection obligations, the Controller shall bear the reasonable costs incurred by Nexis in connection with the inspection.

- 5.2 Nexis shall provide the Controller with all data and information necessary to verify compliance with the obligations set out in this Agreement.

6. Sub-processors

- 6.1 Nexis has the Controller's general written authorization to engage the sub-processors listed in Annex 3. Nexis shall expressly notify the Controller in text form at least 30 days in advance of any intended changes to this list by adding or replacing sub-processors, thereby granting the Controller sufficient time to raise objections to such changes before the relevant sub-processor(s) are engaged. Nexis shall provide the Controller with the necessary information to enable the Controller to exercise their right to object.
- 6.2 Nexis shall ensure that sub-processors are bound by contract to comply with the same data protection obligations as those set out in this Agreement, in particular to implement appropriate technical and organizational measures in accordance with Article 28(4) GDPR.
- 6.3 A list of the sub-processors approved by the Controller at the time of conclusion of this Agreement is set out in Annex 3 (Authorized Sub-processors), which forms an integral part of this Agreement.

7. Start, Contract Period, Termination

- 7.1 This Agreement shall enter into force together with the Main Agreement and, at the latest, upon Nexis's provision of the services in accordance with the Main Agreement.
- 7.2 This Agreement is concluded for the duration of the Main Agreement and shall terminate when the Main Agreement expires or is otherwise terminated early.
- 7.3 Ordinary termination of this Agreement without termination of the Main Agreement is excluded.

8. Legal Consequences of Termination

- 8.1 Upon termination of this Agreement or cessation of the processing services, Nexis shall, at the Controller's choice, return and/or delete all personal data, processing results, and documents containing personal data, unless it is required to retain them under national provisions or Union law.

- 8.2 If the Controller does not make a corresponding choice at or before the termination of this Agreement or the processing services, all personal data shall be deleted, unless there is an obligation to retain the personal data under Union law or the law of the Member States.

9. Miscellaneous

- 9.1 The Parties agree to mutually transfer all rights and obligations under this Agreement, including this transfer obligation, to their respective universal legal successors.
- 9.2 Any amendments, additions, or termination of this Agreement and its annexes, including any deviation from the form stipulated herein, shall be valid only if made in text form (e.g., by e-mail), unless a stricter form, in particular notarization, is required.
- 9.3 The invalidity, illegality, or unenforceability of one or more provisions of this Agreement shall in no way affect the validity, legality, or enforceability of the remaining provisions of this Agreement. Any invalid, void, or unenforceable provision of this Agreement shall – to the extent permitted by law – be deemed replaced by a valid, legal, and enforceable provision that most closely reflects the legal and economic intent pursued by the Parties.
- 9.4 The choice of law and place of jurisdiction shall be determined in accordance with the Nexis 4 Platform Terms and Conditions.

For the Controller:

_____, on _____

Name:

Function:

For Nexis:

_____, on _____

Name:

Function:

Annex 1

Subject Matter of Processing

Subject Matter of the Processing	Technical operation of the NEXIS software
Purpose of Processing	Provision of the NEXIS 4 software in accordance with the Main Agreement
Type of Processing	• Collection (from the Controller's systems) • Storage • Organization • Retrieval • Deletion • Transmission (to the Controller's systems) • Monitoring and logging (recording anomalies and errors) • AI-based analysis, text production and automation
Duration of Processing	In accordance with the term of the Main Agreement
Categories of Personal Data	The categories of personal data processed are determined by the Controller in the course of using our service. In the context of the services provided under the Main Agreement, these regularly include: • First and last name • Business master data (e.g., email address, department,

	location) • Technical information (e.g., IP address) • Identity and access management-related information (e.g., authorization assignments) • Prompt and other textual inputs and outputs
Categories of Data Subjects	Employees of the Controller, business partners of the Controller
Transfer to Third Countries (or International Organizations)	As a general principle, processing is carried out within the European Union / the European Economic Area. Transfers of personal data to third countries or access from third countries cannot be entirely excluded in the context of Microsoft support, security, maintenance, or group services. Such transfers or access shall take place solely on the basis of appropriate safeguards in accordance with Articles 44 et seq. GDPR, in particular an adequacy decision pursuant to Article 45 GDPR, the EU Standard Contractual Clauses pursuant to Article 46 GDPR, and, where applicable, additional supplementary measures.

Annex 2

Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation, as well as the nature, scope, context, and purposes of processing, and the varying likelihood and severity of risks to the rights and freedoms of natural persons, Nexis has implemented the following technical and organizational measures to ensure an appropriate level of protection within the meaning of Article 32 GDPR:

1. Ensuring confidentiality (Art. 32(1)(b) GDPR)	
<i>Entry control</i>	
• Chip cards / transponder systems • Security locks • Securing of building shafts • Doors with knobs on the outside • Key management / inventory list • Reception / front desk / gatekeeper • Visitor log / record of visitors • Employee / visitor ID badges • Visitors accompanied by employees • Careful selection of cleaning services	
<i>Access control</i>	
• Login with username and password • Login with two-factor authentication • Server antivirus software • Client antivirus software • Firewall • Encryption of data carriers • Automatic desktop lock • User authorization concept • Administered user management • Mandatory password requirements • Clean desk policy • Mobile Device Policy • Remote Working Policy	
<i>Logical access control</i>	
• Automated log analysis • Logging of all data access • Logging of application access	

• Granular permissions for data, applications, and operating system • Granular permissions for reading, modifying, and deleting • Data encryption “at rest” • Transport encryption “in transit” • Reduction of administrator access rights • Careful selection of administrators • Management of user rights by administrators
<i>Separation control</i>
• Automated log analysis • Logging of all data access • Logging of application access • Granular permissions for data, applications, and operating system • Granular permissions for reading, modifying, and deleting • Logical separation of tenants • Separation of test and production systems • Reduction of administrator access rights • Careful selection of administrators • Management of user rights by administrators
<i>Pseudonymization</i>
• Pseudonymization of customer data in files, where applicable and technically feasible • Pseudonymization of customer data in NEXIS 4 (analysis software), where applicable and technically feasible
<i>Transfer control</i>
• Strong isolation of the internal network using a secure tunnel (VPN access) • Limited group of employees • Employees trained in information security • Commitment of employees to handle information carefully and maintain confidentiality • Email encryption (S/MIME / PGP) • Use of VPN • Data encryption “at rest” • Transport encryption “in transit” • Documentation of data recipients, retention periods, and security measures • Regular monitoring of data transfers
2. Ensuring integrity and input control (Art. 32(1)(b) GDPR)
• Logging of user actions when entering data • Logging of user actions when modifying data • Logging of user actions when deleting data • Logging of all actions in NEXIS 4 when processing personal data

- Case-specific evaluation of logs
- Logging data entry, modification, and deletion
- Labeling of recorded data
- Dedicated log server
- Overview of programs with access to personal data
- Individual user profiles
- Assignment of rights based on an authorization concept
- Organizational definition of input responsibilities
- Commitment to data secrecy and confidentiality/non-disclosure
- Authorization concept for log access

3. Ensuring the resilience of systems (Art. 32(1)(b) GDPR)

- Load balancing of network components
- Load balancing of services
- Backup processing facilities available
- Redundant uninterruptible power supply (UPS)
- Redundant air conditioning
- Redundant power supply
- Redundant fire suppression systems
- Computer Emergency Response Team (CERT)
- Regular penetration tests
- Regular patching of all systems
- Regular tests of data restoration and documentation of the results
- Regular employee training

4. Ensuring the availability of and procedures for restoring the availability of personal data (Art. 32(1) (b), (c) GDPR)

- Placement of servers in a dedicated server room at the business premises of Nexis GmbH or at the data center provider's facilities
- Fire alarm system (FAS)
- Fire and smoke detection systems
- Waterless fire suppression in the server room
- Temperature and humidity monitoring in the server room
- Air conditioning of the server room
- Lightning and surge protection
- Uninterruptible power supply (UPS)
- Emergency power generator
- Protected power outlets in the server room
- RAID system / disk mirroring
- Video surveillance of the server room
- Alarm notification in case of unauthorized access to the server room
- Backup and recovery concept (documented)
- Regular review of backup measures
- Regular tests of data restoration and logging of the results
- Server rooms located in separate fire compartments

- Storage of backup media in a secure location outside the server room
- No sanitary facilities in or above the server room
- Separate partitions for operating systems and data
- Existing disaster recovery and emergency plan
- Access restriction to the server room
- Regular vulnerability analysis

5. Procedures for the regular review, assessment, and evaluation of the effectiveness of technical and organizational measures (Art. 32(1)(d) GDPR)

- ISMS considering selected requirements of ISO/IEC 27001
- Structured risk management according to ISO/IEC 27001 and BSI
- Regular internal and external audits within the framework of establishing an ISMS according to ISO/IEC 27001
- Data protection management software
- Internal procedure directories are updated at least annually
- Process for reporting new processing procedures
- Selection of privacy-friendly default settings
- Process for involving the data protection officer
- Review of implemented measures according to the PDCA cycle (Plan, Do, Check, Act)
- Process for responding to data protection breaches

6. Order Control

- Contract design according to GDPR (Art. 26, 28 GDPR)
- Centralized recording of existing service providers
- Contract management and regular updating of contracts

7. AI-specific measures

- Server-side invocation of the LLM component via a centralized, encapsulated integration layer; no direct invocation of the LLM provider from the user's browser
- Operation of the local ML component as an internal service without external interfaces
- Tenant-separated management of RAG indices and semantic stores; retrieval exclusively within the respective tenant context
- Server-side assembly of system prompts and tenant-specific prompt components; no user access to system prompts
- No use of customer data, prompts, outputs, or RAG content for the training, fine-tuning, or improvement of foundation models
- No incorporation of RAG content into model weights; no fine-tuning or customer-specific training using customer or personal data without a

separate data protection assessment and contractual basis

- Detection of prompt injection, filtering of malicious input patterns, and validation of input length and structure
- Implementation of a multi-layer system prompt concept for identity, behavior, scope, and security control
- Plausibility checks, schema validation, and output validation of LLM outputs prior to delivery to the user
- Tenant-specific API quotas and rate limiting to prevent misuse and DDoS patterns
- Activation of Azure AI Content Safety to assess inputs and outputs for harmful content at runtime
- Identification of NICO interaction points as AI functionality and visual labeling of AI-generated content
- Display of an informational notice prior to first use, indicating the AI-based nature of the functionality, potential inaccuracies, and user responsibility
- Provision of NICO results as suggestions, hints, summaries, classifications, or findings; users are able to reject, modify, or discard AI-generated suggestions
- Storage of raw prompts only to the extent required for workflow context, traceability, or audit trail purposes; time-based deletion in accordance with customer-configured retention periods

Annex 3

Authorized sub-processors

Sub-processors	Address	Purpose
Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay Dublin 2D02 R296, Ireland	Provision of virtualized infrastructure using the Microsoft Azure platform for the operation of the SaaS application, including the hosting and execution of LLM/AI models within the Azure environment.
Nexis GRC GmbH	Hans-Henny-Jahnn-Weg 53, 22085 Hamburg	Provision of support and consulting services to customers, the provision of the software application, and the operation of the hosting and IT Infrastructure required for such purposes.
Nexis Group GmbH	Rudolf-Vogt-Straße 6, 93053 Regensburg	Monitoring, development, and continuous improvement of the services provided.