Data Processing Agreement (DPA) Nexis QSEC (SaaS)

Annex 1 to the QSEC Platform GTC – Data Processing Agreement (the "Agreement"), Version 1.4

As of: November 16, 2026 | **Status:** Convenience translation

Table of Contents

1. Subject Matter of the Processing 1
2. Processing Only on the Controller's Instructions 2
3. Confidentiality 2
4. Security of Processing 2
5. Obligations to Provide Information and Rights of Inspection 3
6. Sub-processors 3
7. Start, Term, Termination 3
8. Legal Consequences of Termination 4
9. Miscellaneous 4
Annex 1 5
Annex 2 6
Annex 3 8

Please note: This English version of the Data Processing Agreement is a convenience translation only. In case of conflicts between the German and the English version, the German version shall prevail.

Hereinafter, the Controller and Nexis shall each be referred to as a "Party" and collectively as the "Parties". 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 QSEC Platform GTC and in connection with the related offer (the "Main Agreement").

Unless otherwise defined in this Agreement, the definitions set forth in the QSEC Platform GTC shall continue to apply equally.

1. Subject Matter of the Processing

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 organisation. 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 organisational measures implemented by Nexis pursuant to Article 32 GDPR are set forth in Annex 2 (Technical and Organisational 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 organisational 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 it 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.

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 authorisation 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 its 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 organisational 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 (Authorised Sub-processors), which forms an integral part of this Agreement.

7. Start, Term, 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 undertake 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 email), unless a stricter form, in particular notarisation, 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 purpose pursued by the Parties.

9.4 The choice of law and place of jurisdiction shall be determined in accordance with the QSEC Platform GTC.

For the Controller:	**For Nexis:**
Name:	Name:
Function:	Function:

Annex 1

Subject Matter of the Processing

Subject matter of the processing	Technical operation of the QSEC software
Purpose of the processing	Provision of the QSEC software in accordance with the Main Agreement
Type of processing	• Collection (from the Controller's systems) • Storage • Organisation • Retrieval • Deletion • Transmission (to the Controller's systems) • Monitoring and logging (recording of anomalies and errors)
Duration of the 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. authorisation assignments)
Categories of data subjects	Employees and contact persons of the Controller
Transfer to third countries (or international organisations)	As a general principle, processing is carried out within the European Union / the European Economic Area. Transfers to third countries or access from third countries cannot be entirely excluded in the context of Microsoft support, security, maintenance or group services and shall take place solely on the basis of appropriate safeguards in accordance with Articles 44 et seq. GDPR, in particular an adequacy decision, EU Standard Contractual Clauses and supplementary measures.

Annex 2

Technical and Organisational 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 organisational measures to ensure an appropriate level of protection within the meaning of Article 32 GDPR:

Appendix A – Technical and organisational measures of the processor (Art. 32 GDPR)

Ensuring confidentiality and pseudonymisation and encryption of personal data

Entry control

- Entry to rooms only possible with a key
- Management of entry (issuing of keys, entry to rooms, etc.)
- Limited group of employees

Access control

- Centralised management of users and clients by the system administrator
- Password policy incl. password length, password change
- Authentication with username / password
- Strong isolation of the internal network using a secure tunnel (VPN access)
- Use of anti-virus software on clients and servers
- Use of multi-level firewalls in the network
- Use of hard disk and data carrier encryption in accordance with the current state of the art on clients and servers
- Use of TLS/SSL encryption of internal and, where applicable, external communication channels
- Regular installation of security updates on clients and servers
- Dedicated instance for the email service on an isolated virtual server

Logical access control

- Password policy incl. password length, password change
- Additional data encryption of strictly confidential information, if necessary
- Secure storage of backups
- Management of permissions by the system administrator

Separation control

- Database permissions
- Use of virtualised separation per internal application
- Logical separation of customer files

Pseudonymisation

- Pseudonymisation of customer data in files, where applicable and technically feasible

Transfer control

- Strong isolation of the internal network using a secure tunnel (VPN access)
- Limited group of employees
- Employees trained in information security and data protection
- Commitment of employees to handle information carefully and to maintain confidentiality

Ensuring integrity & input control

- Restriction of entry, access and logical access to information (see item 1)
- Backup and restore processes to restore integrity
- Logging of user actions when entering data
- Logging of user actions when modifying data
- Logging of user actions when deleting data
- Case-specific evaluation of logs

Ensuring the resilience of systems

- Testing of resilience
- Monitoring of systems

Ensuring availability and procedures for restoring the availability of personal data after a physical or technical incident

- Fire alarm system (FAS)
- Fire extinguishers
- Backup and restore processes
- Testing of data recovery
- Central storage of information on servers

Procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organisational measures / effectiveness control

- Establishment of an ISMS according to 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
- Audits in the context of data protection and the requirements of the GDPR
- Data protection management within the framework of establishing the ISMS

Order control

- Documentation of processing activities in the record of processing activities
- Use of sub-processors exclusively in accordance with Section 6 and Annex 3
- Processing of personal data exclusively on the basis of written instructions
- Commitment of the processor's employees to confidentiality

Annex 3

Authorised Sub-processors

Sub-processor	Address	Purpose
PlusServer GmbH	Venloer Str. 47, 50672 Köln	Provision of the virtualised hardware for SaaS operation
Nexis GmbH	Rudolf-Vogt-Straße 6, 93053 Regensburg	Provision of support and consulting services to customers, provision of the software application and operation of the hosting and IT infrastructure required for this purpose
Nexis Group GmbH	Rudolf-Vogt-Straße 6, 93053 Regensburg	Monitoring, development and improvement of the services provided