

Annex 2

Technical and organizational measures

Taking into account the state of the art, the implementation costs, as well as the nature, scope, circumstances and purposes of the processing, as well as the different probability and severity of the risks to the rights and freedoms of natural persons, Nexis has implemented the following technical and organisational measures to ensure an adequate level of protection within the meaning of Article 32 DSGVO:

1. Guarantee of confidentiality (Art. 32 para. 1 lit. b DSGVO)	
Access control	• Chip Cards / Transponder Systems • Security locks • Securing the building shafts • Doors with knob on the outside • Key regulation / list • Reception / Reception / Doorman • Visitors' book / visitors' log • Employee / visitor badges • Visitors accompanied by staff • Care in choosing cleaning services
Access control	• Login with username & password • Login with 2-factor authentication • Anti-Virus Software Server • Anti-Virus Software Clients • 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
Access control	• Automated log evaluation • Logging of all data accesses

- Logging of application accesses
- Differentiated permissions Data, applications, operating system
- Read, modify, delete fine-grained permissions
- Data encryption "at rest"
- Transport encryption "in transit"
- Reduction of administrator access
- Care Selection Administrators
- Management of user rights by administrators

Separation control

- Automated log evaluation
- Logging of all data accesses
- Application Access Logging
- Differentiated permissions Data, applications, operating system
- Read, modify, delete fine-grained permissions
- Client separation logical
- Separation of test and production systems
- Reduction of administrator access
- Care Selection Administrators
- Management of user rights by administrators

Pseudonymization

- Pseudonymization of customer data in files, if applicable and technically feasible
- Pseudonymization of customer data in NEXIS 4 (analysis software), if applicable and technically feasible

Transfer control

- Strong isolation of the internal network with the help of a secure tunnel (VPN access)
- Limited group of employees
- Employees trained in information security
- Obligation of employees to handle information carefully and to maintain confidentiality
- Email encryption (S/MIME / PGP)
- Use of VPN
- Data encryption "at rest"
- Transport encryption "in transit"
- Documentation of data recipients, storage period and security measures
- Regular control of data transmissions

2. Ensuring integrity and input control (Art. 32 para. 1 lit. b DSGVO)

- Logging of user actions when data is entered

- Logging of user actions when data changes
- Logging of user actions when data is deleted
- Logging of all actions in NEXIS 4 when processing personal data
- Needs-based evaluation of the protocols
- Logging of data entry, modification and deletion
- Marking of Collected 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 submission responsibilities
- Commitment to data secrecy or confidentiality/secrecy
- Authorization concept for log access

3. Ensuring the resilience of systems (Art. 32 para. 1 lit. b DSGVO)

- Load balancing of network components
- Load balancing of services
- Alternative processing facilities available
- Redundant UPS
- Redundant air conditioning
- Redundant power supply
- Redundant firefighting
- Computer Emergency Response Team (CERT)
- Regular penetration tests
- Regular patching of all systems
- Regular tests for data recovery and logging of results
- Regular training of employees

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

- Placement of servers in a specific server room in the business premises of Nexis GmbH or the provider of the data center
- Fire alarm system (BMA)
- Fire and smoke alarm systems
- Waterless firefighting in the server room
- Temperature and humidity monitoring server room
- Air conditioning of the server room
- Lightning and surge protection
- Uninterruptible power supply (UPS)
- Emergency power generator
- Protective sockets Severraum
- RAID System / Disk Mirroring

- Video surveillance server room
- Alarm message in case of unauthorized access to the server room
- Backup & Recovery concept (formulated)
- Regular monitoring of back-up measures
- Regular tests for data recovery and logging of results
- Server rooms in different fire compartments
- Store backup media in a secure location outside the server room
- No sanitary connections in or above the server room
- Separate partitions for operating systems and data
- Existing disaster or emergency plan
- Access restriction to the server room
- Regular vulnerability analysis

5. Procedure for regularly reviewing, evaluating and evaluating the effectiveness of technical and organisational measures (Art. 32 para. 1 lit. d DSGVO)

- ISMS taking into account selected requirements of ISO/IEC 27001
- Structured risk management according to ISO/IEC 27001 and BSI
- Regular internal and external audits as part of the establishment of an ISMS according to ISO/IEC 27001
- Privacy Management Software
- Internal process directories are updated at least once a year.
- Process for notifying new processing methods
- Selection of privacy-friendly preferences
- Process for the involvement of the data protection officer
- Review of the measures taken according to the PDCA cycle (Plan, Do, Check, Act)
- Data breach response process

6. Order control

- Drafting of contracts in accordance with the DSGVO (Art. 26, 28 DSGVO)
- Central recording of existing service providers
- Contract management and regular updating of contracts