

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

to the DPA pursuant to Art. 28(3)(b) and (c) and Art. 32 GDPR

Convenience translation. Only the German version is legally binding.

1. Objective, scope, updates

1.1 These TOMs ensure a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing (Art. 32 GDPR).

1.2 The TOMs apply to all WISNOTS services within the scope of processing on behalf, in particular receiving and preparing case data, submission to competent bodies, handling queries, and storing and providing the case status.

1.3 WISNOTS may develop the TOMs further, provided the level of protection is not reduced. They are reviewed at least annually and for cause.

2. Access control and authentication

2.1 Role and authorisation concept

- Role-based access control (RBAC)
- Least-privilege and need-to-know principle
- Separation of duties for privileged activities, where organisationally sensible
- Tenant separation: case data of different controllers is logically separated; access across tenant boundaries is impossible

2.2 Authentication

- Multi-factor authentication for administrative and privileged access
- Secure handling of passwords and credentials
- Authentication of the Controller's users by one-time code sent to the stored email address

2.3 Administrative access and network

- Access to administrative systems only through secured channels
- Segmentation of sensitive administration interfaces

2.4 Joiner/Mover/Leaver

- Defined process for granting, changing and revoking access rights
- Prompt blocking on offboarding or change of role

3. Handling of access credentials for third-party portals

3.1 The Controller's access credentials for installer registers and grid operators' portals are stored encrypted in a dedicated secret store and are never stored or logged in plain text.

3.2 Access is restricted to authorised persons, takes place exclusively for handling specific cases and is logged.

3.3 The Controller may change access credentials itself or request their deletion at any time. Deletion takes place without delay.

3.4 Access credentials are not passed on to third parties and are not stored in backups outside the secret store.

4. Data fields requiring special protection

4.1 Fields with increased protection needs, in particular bank details, date of birth and tax identification number, are only collected where the competent body requires them.

4.2 Access to these fields is restricted to the persons required for case handling and is logged separately.

5. Logging, traceability, monitoring

5.1 Logging

- Logging of security-relevant events (authentication, administrative actions, access to case data, critical system events)
- Protection of logs against manipulation, where technically and organisationally possible

5.2 Log retention

- Retention only as long as necessary for security and evidence purposes
- Guideline: generally up to 12 months; adjusted according to risk, legal requirements or the Controller's instructions

5.3 Monitoring: central monitoring and alerting to detect anomalies and security-relevant events

6. Encryption and key management

6.1 In transit: transport encryption in line with the state of the art (TLS 1.3, at least TLS 1.2)

6.2 At rest: encryption in line with the state of the art (AES-256 or equivalent)

6.3 Key management

- Key management through suitable mechanisms (KMS or equivalent)
- Access to key material strictly restricted and logged
- Key rotation regularly and for cause, guideline at least annually and after security incidents

6.4 Data minimisation: only the data required for submission to the competent body is collected and stored.

7. Backup, recovery, availability

7.1 Backups

- Regular backups according to the backup concept, guideline daily
- Protection against unauthorised modification, where available
- Storage exclusively within the European Union (Convex, AWS eu-west-1, Ireland)

7.2 Recovery: guideline RTO 24 hours, RPO 24 hours

7.3 Restore tests: recoverability is tested at appropriate intervals, guideline at least annually and for cause

8. Vulnerability management and secure development

8.1 Vulnerability management

- Regular vulnerability analyses, at least annually, more often depending on risk
- Prioritised remediation of critical findings within reasonable periods

8.2 Patch and update management: security updates are applied promptly on a risk basis

8.3 Secure development

- Code reviews under the four-eyes principle, where practicable

- Secrets management: no credentials or keys in code
- Separation of development, test and production environments
- No productive personal data is used in test and development environments

9. Incident response

9.1 Documented process including roles and responsibilities (detection, containment, remediation, follow-up)

9.2 Security-relevant incidents are handled without delay once known. Personal data breaches are reported to the Controller in accordance with the DPA, guideline within 48 hours of becoming aware

9.3 Root cause analysis and action plan, guideline within 30 days

10. Personnel and organisation

10.1 Persons with access to personal data are bound to confidentiality

10.2 Regular data protection and security training, guideline annually

10.3 Regular review of privileged authorisations and prompt revocation of rights no longer required

11. Sub-processors

- Engagement only in accordance with the DPA
- Contractual obligation to equivalent data protection obligations under Art. 28(4) GDPR
- Third-country transfers only in compliance with Art. 44 et seq. GDPR
- Current status see Annex 3

12. Deletion and return

- Return or deletion of personal data after termination in accordance with the DPA
- Deletion in line with the state of the art (secure deletion, cryptographic erasure, key destruction)
- Backups: deleted as part of the rolling backup concept; until then no productive use, access strictly restricted

13. AI processing

- Use of Requesty's EU endpoint in Frankfurt am Main only; redirection to any other endpoint is technically impossible
- Use of approved model deployments in EU regions only; the endpoint rejects requests to non-approved models, with no fallback to other models
- No logging or caching of request content at Requesty (zero data retention)
- No use of case data for training AI models
- The model used for each processing step is recorded in the case

Berlin, 28 September 2026

WISNOTS GmbH