COMPLIANCE REPORT

NetTools Suite

Report Coverage:

- Open Source License Compatibility
- Commercial Use Assessment
- GDPR (DSGVO) Compliance
- NIS2 Security Considerations

Report Date: December 17, 2025

Version: 1.0

1. Executive Summary

This compliance report analyzes NetTools Suite for suitability as an open source project, commercial use licensing compatibility, GDPR (DSGVO) compliance, and NIS2 security requirements.

Category	Status	Summary
Open Source License	APPROVED	MIT License - fully compatible
Commercial Use	PERMITTED	All dependencies allow commercial use
GDPR Compliance	OK	Local-only tool, no PII collection
NIS2 Security	INFO	Depends on organizational policies

Overall Assessment

NetTools Suite is SUITABLE for open source distribution under the MIT License. All dependencies use permissive licenses compatible with commercial use.

2. License Analysis

2.1 Project License

NetTools Suite is licensed under the MIT License, which is permissive and business-friendly. It allows commercial use, modification, and distribution with only attribution required.

2.2 Permissive Licenses (No Restrictions)

Package	License	Purpose
customtkinter	MIT	GUI Framework
Pillow	MIT-CMU	Image Processing
pythonping	MIT	Network Ping Operations
requests	Apache 2.0	HTTP Client Library
cryptography	Apache 2.0 / BSD-3	Encryption Functions
urllib3	MIT	HTTP Library
beautifulsoup4	MIT	HTML Parsing
speedtest-cli	Apache 2.0	Internet Speed Testing
matplotlib	PSF	Data Visualization
numpy	BSD	Numerical Computing

2.3 PyInstaller GPL Consideration

Important: PyInstaller Exception

PyInstaller is licensed under GPLv2, but has a special bootloader exception that allows bundling proprietary/MIT code. Applications built with PyInstaller do NOT inherit the GPL license. Your application remains under its own license (MIT).

APPROVED PyInstaller exception clause permits MIT-licensed distribution

3. GDPR (DSGVO) Compliance

3.1 Data Processing Overview

NetTools Suite is primarily a LOCAL network diagnostic tool. The following data handling characteristics were identified during code review:

3.2 Local Data Storage

- Window geometry and UI preferences stored in ~/.nettools_config.json
- Theme settings and favorite tools (user preferences only)
- Enabled/disabled tool preferences
- Scan history and comparison data (local files only)
- Network profiles containing IP ranges and scan configurations

OK All data stored locally - No cloud transmission

3.3 External Network Connections

The application MAY connect to external services for specific features (all user-initiated):

- speedtest-cli: Connects to Speedtest.net servers for speed tests
- MXToolbox API: Optional DNS lookup enhancement (requires user API key)
- DNSDumpster: Optional domain reconnaissance (requires user API key)
- phpIPAM: Optional IPAM integration (user-configured server)

GDPR Risk Assessment: LOW

No automatic collection of Personal Identifiable Information (PII). No telemetry, analytics, or tracking. No data transmission without explicit user action. All data remains local.

4. NIS2 Security Considerations

4.1 Overview

The NIS2 Directive is an EU regulation for improving cybersecurity. As a diagnostic tool, NetTools Suite itself is not directly subject to NIS2. However, organizations using it may be.

4.2 Security Features

- Open source: Full code transparency and auditability
- Local execution: No cloud dependencies, reduced attack surface
- No network listeners (except iPerf server mode when explicitly used)
- Configurable features: Sensitive tools can be disabled via settings
- Remote Tools module: Currently DISABLED by default

4.3 Recommendations for Enterprise Use

- Deploy via approved software channels only
- Restrict access to authorized network administrators
- Enable logging if using in regulated environments
- Review and approve external API integrations before use
- Keep Remote Tools disabled unless specific need exists
- Encrypt or protect exported scan results

NIS2 Compliance Note

Tool compliance depends on organizational deployment policies. The tool itself has good security characteristics suitable for enterprise use.

5. Recommendations

5.1 Required for Open Source Release

- Include LICENSE.txt (MIT) in all distributions [DONE]
- Add attribution notices for third-party libraries
- Document external API dependencies clearly

5.2 Recommended Improvements

- Add SECURITY.md file for vulnerability reporting
- Create CONTRIBUTING.md for contributor guidelines
- Add api_keys.json to .gitignore (sensitive data)
- Provide api_keys.example.json template [DONE]
- Consider code signing for distributed executables

6. Conclusion

NetTools Suite has been thoroughly analyzed for compliance with open source licensing, GDPR regulations, and NIS2 security requirements.

Final Verdict: APPROVED FOR OPEN SOURCE DISTRIBUTION

1. OPEN SOURCE: Fully compatible with MIT License distribution.
2. COMMERCIAL USE: Permitted without licensing restrictions.
3. GDPR: Low risk - local tool with no PII collection.
4. NIS2: Good security posture suitable for enterprise deployment.

A. Appendix: Complete License List

Package	License	Compatibility
altgraph	MIT	Permissive
bcrypt	Apache 2.0	Permissive
beautifulsoup4	MIT	Permissive
certifi	MPL 2.0	File-level copyleft
cryptography	Apache 2.0 / BSD-3	Permissive
customtkinter	MIT	Permissive
dnspython	ISC	Permissive
matplotlib	PSF	Permissive
numpy	BSD	Permissive
Pillow	MIT-CMU	Permissive
PyInstaller	GPLv2 (Exception)	Bootloader exception
pythonping	MIT	Permissive
requests	Apache 2.0	Permissive
speedtest-cli	Apache 2.0	Permissive
urllib3	MIT	Permissive