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.

OVERALL ASSESSMENT: NetTools Suite is SUITABLE for open source distribution under the MIT License.

OK	Open Source License Compatibility: APPROVED
OK	Commercial Use: PERMITTED (with minor considerations)
OK	GDPR Compliance: LOW RISK (local-only tool)
INFO	NIS2: INFORMATIONAL (user responsibility)

1. Executive Summary

2. License Analysis for Open Source Distribution

2.1 Project License

NetTools Suite is licensed under the MIT License, which is:

- Permissive and business-friendly

- Compatible with most open source licenses

- Allows commercial use, modification, and distribution

- Requires only attribution in derivative works

2.2 Dependency License Summary

PERMISSIVE LICENSES (No Restrictions):

- customtkinter: MIT - GUI Framework

- Pillow: MIT-CMU - Image Processing

- pythonping: MIT - Network Ping

- requests: Apache 2.0 - HTTP Client

- cryptography: Apache 2.0 / BSD-3 - Encryption

- urllib3: MIT - HTTP Library

- beautifulsoup4: MIT - HTML Parsing

- speedtest-cli: Apache 2.0 - Speed Testing

COPYLEFT LICENSES (Special Considerations):

- PyInstaller: GPLv2 - Build Tool - SPECIAL CONSIDERATION

OTHER PERMISSIVE LICENSES:

- matplotlib: PSF - Plotting - Python Software Foundation

- certifi: MPL 2.0 - SSL Certificates

2.3 P

PyInstaller is licensed under GPLv2. However, according to PyInstaller's official FAQ:

- The PyInstaller bootloader has a special exception that allows bundling proprietary code

- Applications built with PyInstaller do NOT inherit the GPL license

- Your application remains under its own license (MIT in this case)

CONCLUSION: PyInstaller's GPL does NOT affect NetTools Suite's MIT license.

| OK | PyInstaller: Exception clause permits MIT-licensed distribution |

2.4 Commercial Use Assessment

All dependencies used by NetTools Suite permit commercial use:

- MIT License: Unrestricted commercial use

- Apache 2.0: Permits commercial use with patent grants

- BSD: Permits commercial use with attribution

- PSF: Python Software Foundation license permits commercial use

- MPL 2.0: File-level copyleft only, compatible with commercial use

CONCLUSION: NetTools Suite can be used commercially without licensing conflicts.

OK	Commercial Use: FULLY PERMITTED

3. GDPR (DSGVO) Compliance Analysis

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

Data stored LOCALLY on the user's machine:

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

3.3 External Network Connections

The application MAY connect to external services for specific features:

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

3.4 Sensitive Data Handling

The following sensitive data may be processed:

- IP addresses: Network diagnostic purpose (no PII)
- Hostnames: Network diagnostic purpose (no PII)
- API Keys: Stored in local api_keys.json file
- Remote credentials (PSExec - DISABLED): Username/password for remote access

3.5 GDPR Risk Assessment

RISK LEVEL: LOW

Justification:
- No automatic collection of Personal Identifiable Information (PII)
- No telemetry, analytics, or tracking functionality
- No data transmission to third-party servers without user action
- All data remains on the local machine
- External API usage is optional and user-configured

RECOMMENDATION: No GDPR compliance documentation required for the tool itself. Organizations using the tool should assess their own data handling policies.

| OK | GDPR Compliance: LOW RISK - Local tool, no PII collection |

4. NIS2 Security Considerations

4.1 NIS2 Overview

The NIS2 Directive (Network and Information Security Directive 2) is an EU regulation for improving cybersecurity. As a network diagnostic TOOL, NetTools Suite itself is not directly subject to NIS2. However, organizations using it may be.

This section provides security considerations for organizations deploying the tool.

4.2 Security Features

Positive security characteristics:

- Open source: Full code transparency and auditability
- Local execution: No cloud dependencies reduce attack surface
- No network listeners: Tool does not open server ports (except iPerf when used)
- Configurable features: Sensitive tools can be disabled via settings

4.3 S

Areas requiring user attention:

- API Keys: Store api_keys.json securely, consider encryption
- Remote Tools (DISABLED): Module handles credentials - keep disabled unless needed
- phpIPAM Integration: Uses network credentials - ensure SSL/TLS
- Scan Results: May contain sensitive network topology - protect exports

4.4 R

For NIS2-compliant organizations:

- 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

INI

5. Recommendations for Open Source Release

5.1 Required Actions

- Include LICENSE.txt (MIT) in all distributions - DONE

- Add attribution notices for third-party libraries in documentation

- Document external API dependencies clearly

5.2 R

- Add SECURITY.md file for vulnerability reporting

- Create CONTRIBUTING.md for contributor guidelines

- Add CHANGELOG.md for version history

- Consider removing api_keys.json from repository (add to .gitignore)

- Add example configuration file (api_keys.example.json)

5.3 O

- Add code signing for distributed executables

- Create privacy policy document for enterprise users

- Implement optional audit logging feature

6. Conclusion

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

KEY FINDINGS:

1. OPEN SOURCE: The tool is FULLY COMPATIBLE with open source distribution under MIT License. All dependencies use permissive licenses that allow commercial and open source use.

2. COMMERCIAL USE: The tool CAN be used commercially without licensing restrictions. PyInstaller's GPL exception explicitly permits this.

3. GDPR: The tool presents LOW RISK for GDPR compliance as it is a local-only tool that does not collect, process, or transmit Personal Identifiable Information.

4. NIS2: As a diagnostic tool, NIS2 compliance depends on organizational deployment policies. The tool itself has good security characteristics suitable for enterprise use.

OVERALL RECOMMENDATION: NetTools Suite is APPROVED for open source release and commercial deployment with the minor recommendations noted in Section 5.

OK	APPROVED FOR OPEN SOURCE DISTRIBUTION

Appendix A: Complete License List

altgraph	MIT
annotated-types	MIT
anyio	MIT
bcrypt	Apache 2.0
beautifulsoup4	MIT
certifi	MPL 2.0
cffi	MIT
charset-normalizer	MIT
click	BSD-3-Clause
contourpy	BSD
cryptography	Apache 2.0 / BSD-3
customtkinter	MIT
cycler	BSD
darkdetect	BSD
dnspython	ISC
fonttools	MIT
idna	BSD-3-Clause
kiwisolver	BSD
matplotlib	PSF
numpy	BSD
packaging	Apache 2.0 / BSD
Pillow	MIT-CMU
pycparser	BSD
PyInstaller	GPLv2 (Exception)
pyparsing	MIT
pythonping	MIT
requests	Apache 2.0
speedtest-cli	Apache 2.0
urllib3	MIT