Rogue

data protection policy

Rogue Cybersecurity AS is dedicated in safeguarding the privacy and security of personal and sensitive data related to our consultancy services and projects. This Data Protection Policy outlines how Rogue can collect, use, store, and protect information, ensuring compliance with applicable laws and regulations, and maintaining the trust of Rogue's clients and business partners. Last revised 16-06-2024, by Theodore Grødahl.

1. Scope

This policy applies to all employees, contractors, and third parties who handle data on behalf of Rogue Cybersecurity AS, particularly in relation to network diagrams, IP addresses, logs, telemetry data, and attachments for support cases.

2. Data Collection

We collect only the data necessary for providing cybersecurity consultancy services, including:

- Network diagrams
- IP addresses
- System and application logs
- Accounts and credentials
- Telemetry, attachments and documentation for support cases
- Personal identification information (name, email, phone number, etc.)

3. Data Usage

Collected data is used for:

- Providing and improving cybersecurity support
- Analyzing and addressing security incidents
- Providing better future communicating with you (the client)
- Administrative and billing purposes
- Ensuring compliance and SLA expectations

4. Data Storage

Data is stored securely in Rogue's cloud-storage, protected by industry-standard encryption, access controls, and other security measures. Only authorized personnel have access to sensitive data, and any access is logged.

5. Data Retention

- Active Data: Personal and consultancy-related data will be retained as long as it is actively used for business operations.
- Inactive Data: Personal and consultancy-related data that has not been used for 180 days will be identified as inactive. Inactive data will be securely deleted to ensure data protection and compliance with our retention policy.

data protection policy

6. Data Protection Rights

Individuals and clients have the right to:

- Access their personal and consultancy-related data
- Request correction of inaccurate data
- Request deletion of data that is no longer necessary
- Object to or restrict the processing of their data
- Withdraw consent for data processing

7. Data Security Measures

To protect personal and consultancy-related data, Rogue implements the following security measures:

- Encryption of data in transit and at rest
- Regular security audits and vulnerability assessments
- Employee training on data protection and security practices
- Access controls to limit data access to authorized personnel only

8. Non-Disclosure

All employees, contractors, and third parties are required to sign a non-disclosure agreement (NDA) to protect confidential information, including network diagrams, IP addresses, logs, and other sensitive data. Unauthorized disclosure of such data is prohibited and will result in disciplinary action.

9. Data Breach Response

In the event of a data breach:

- We will promptly identify and contain the breach
- Affected individuals and clients will be notified without undue delay (up to 72 hours)
- We will conduct a thorough investigation to determine the cause and prevent future breaches

10. Policy Updates

This policy will be reviewed annually and updated as necessary to ensure compliance with relevant laws and best practices. Any changes to the policy will be communicated to all employees and relevant stakeholders.

Contact Information

For questions or concerns regarding this policy or data protection practices, please contact Rogue DPO at: dpo@rogue.no

By adhering to this Data Protection Policy, Rogue Cybersecurity AS aims to protect personal and consultancy-related data effectively and maintain trust with our clients and partners.