Technical and Organizational Measures

Last updated 30.10.2026.

1. Introduction & Purpose

This document outlines the Technical and Organizational Measures (TOMs) implemented by superhack to safeguard the secure operation of our platform and to protect the confidentiality, integrity, and availability of the information entrusted to us by our customers. It supports compliance with relevant laws and regulations, including the German Federal Data Protection Act (BDSG) and the EU General Data Protection Regulation (GDPR), particularly Article 32, which mandates appropriate technical and organizational measures to protect data.

---

2. Scope

The measures outlined in this document apply to superhack's internal processes and to the operation of the superhack platform, including the customer data and the testing data we process when delivering our services. The scope covers superhack's internal systems, the platform infrastructure, the data our AI agents gather from customer systems during authorized testing, and any third-party systems used as part of service delivery.

---

3. Roles & Responsibilities

superhack and its customers share the goal of improving the customer's security, but responsibility is clearly divided. superhack is responsible for the secure operation of its platform and for protecting the information entrusted to it; customers are responsible for acting on the findings and insights that superhack provides.

- **superhack**: Is responsible for the secure operation of the platform and everything connected to it, and for safeguarding the confidentiality, integrity, and availability of the information entrusted to us — including the vulnerabilities and findings our AI agents discover in customer systems. We deliver these findings, together with context and remediation guidance, through the platform.
- **Customers**: Retain full responsibility for their own environments, systems, and data. superhack identifies and surfaces security weaknesses, but it does not remediate them. Customers are responsible for handling the findings and insights we provide responsibly and confidentially, prioritizing them, and driving the identified issues through to remediation — as well as for meeting their own regulatory and compliance obligations.

4. Organizational and Technical Measures

superhack employs a comprehensive blend of organizational and technical controls to secure its applications, systems, and information, and everything connected to the operation of the platform and the data we process on behalf of our customers.

4.1 Security Governance & Policies

- **Governance**: Security oversight is managed by our Managing Director(s), ensuring that superhack consistently adheres to its own high standards.
- **Policies**: superhack implements strict internal security policies, covering topics such as incident management, access control, and data security. We hold our own operations to the same rigorous security standards that our platform helps our customers achieve, ensuring alignment with best practices and demonstrating our commitment to security excellence.

4.2 Staffing and Security

- **Trusted Employees**: superhack exclusively works with employed personnel, ensuring that everyone involved in operating the platform and delivering our services is well-trained, accountable, and fully integrated into our internal security processes.
- **Limited Use of Freelancers**: superhack does not typically engage freelancers in the delivery of its services. If demand arises and external resources are required, freelancers are only brought in under explicit controls and agreements, ensuring that they meet the same rigorous security standards as our employees.
- **Background Checks**: Employees undergo background checks when required by regulatory standards or customer agreements, ensuring trustworthiness and adherence to security protocols.
- **Small, Contained Team**: superhack operates as a small, contained team, allowing for tighter oversight and higher control over all security-related activities, ensuring the quality and confidentiality of all services provided.
- **Employee Training**: Adequate training on data protection, secure coding, and incident response ensures all employees follow best practices.

4.3 Data Processing

superhack follows a strict principle of data minimization, ensuring that only the minimum amount of data necessary to deliver its services is accessed or handled. This includes:

- **As-Needed Data Access**: superhack accesses customer systems only within the scope the customer authorizes for testing, limiting access to what is essential for the agreed engagement.

- **Purpose Limitation**: Data is accessed solely for the purposes agreed upon during any engagement, and we avoid requesting or handling any extraneous information that is not relevant to the services being provided.
- **Data Handling and Retention**: Customer data is handled with the utmost care, and only the minimum amount of data required for the successful completion of the engagement is retained. Once the engagement is completed, data is securely deleted or returned to the customer as per the agreed terms.

4.4 Access Control

- **Least Privilege & RBAC**: superhack enforces least-privilege access across all internal and customer systems.
- **Phishing-Resistant Multi-Factor Authentication (MFA)**: MFA, utilizing strong, phishing-resistant methods such as passkeys or FIDO2/WebAuthn, is required for accessing sensitive systems and data. This ensures a higher level of security by mitigating risks associated with traditional password-based authentication.
- **Customer Data Separation**: superhack ensures strict separation of customer data at the access management level. Access to customer environments and data is segregated, with each customer's data being isolated to prevent cross-access or unintended exposure between customers. This ensures that only authorized personnel with specific roles can access each customer's data.
- **Access Reviews**: Periodic reviews of access rights ensure that access levels are appropriate to current roles and responsibilities.

4.5 Encryption & Data Protection

- **Data Encryption**: superhack ensures that all sensitive data is encrypted both at rest and in transit using industry-standard encryption protocols.
- **Workplace Device Encryption**: All workplace devices used for data processing are encrypted at the operating system level to protect against unauthorized access, ensuring that sensitive data remains secure even if the device is compromised.
- **SaaS Applications**: For any SaaS applications used by superhack, we ensure that these services implement up-to-date security measures, including encryption for data both in transit and at rest.
- **IaaS/PaaS Encryption**: When utilizing IaaS or PaaS environments, superhack employs readily available encryption methods to secure customer data and maintain compliance with security best practices.
- **Backup Encryption**: All backups of customer data are encrypted using asymmetric encryption to provide an additional layer of security, ensuring that backup data is secure and cannot be accessed without the appropriate private keys.

- **Pseudonymization/Anonymization**: Where applicable, superhack anonymizes or pseudonymizes (customer-)data to further reduce the risk of exposure in the unlikely event of a security breach.

4.6 Incident Management & Response

- **Incident Detection & Monitoring**: superhack continuously monitors its internal systems for security incidents and indicators of compromise.
- **Response Plans**: A formal incident response plan ensures quick and effective mitigation of threats.
- **Incident Communication**: Customers are notified promptly of any incidents affecting their systems or data, with clear reporting timelines.

4.7 Third-Party Vendor Management

- **Vendor Risk Assessments**: All third-party vendors (particularly SaaS, IaaS, PaaS etc.) undergo a security assessment to ensure their controls meet superhack's standards.
- **Contractual Security Requirements**: Security requirements are built into all vendor contracts to mitigate risk and maintain the compliance chain.
- **Monitoring of Third-Party Services**: Vendors are regularly assessed for continued compliance with security standards, and their access to customer data is tightly controlled.

4.8 Generative AI Tool Usage

- **Risk Awareness**: superhack recognizes the emerging risks associated with the use of Generative AI tools, such as inadvertent data leakage, intellectual property risks, and the potential for creating vulnerable outputs. These tools can unintentionally expose sensitive customer data or create code that is not security-hardened.
- **Compliant AI Tools**: superhack uses only Generative AI tools and Large Language Models (LLMs) that comply with data protection standards, ensuring contractual certainty that any data provided is not used for training purposes or other exploitation. We ensure that the tools used meet strict security and privacy requirements, protecting customer data from misuse.
- **Training and Policies**: superhack ensures that employees are trained on the risks associated with AI tools, with strict policies governing their usage. Employees are prohibited from inputting confidential or sensitive information into publicly accessible AI systems.
- **Review & Mitigation**: Any outputs generated by AI tools are carefully reviewed by security experts to ensure they meet security standards before being integrated into customer solutions. This ensures that the use of AI does not introduce security vulnerabilities.

4.9 Modern Security Tools & Technologies

superhack utilizes a range of advanced security tools and technologies to ensure a robust security posture across all systems and customer engagements. These tools are integral to our technical measures and include:

- **Agentic Hacking with superhack**: We use superhack against ourselves. The same agents that test our customers' attack surfaces test our own platform and infrastructure, and their findings are remediated and retested.
- **Password Management**: superhack implements secure password management solutions, including password vaults, for both internal and customer-related credentials, ensuring the use of strong passphrases and secure storage thereof.
- **Endpoint Detection and Response (EDR)**: We use advanced EDR solutions to detect, monitor, and respond to threats on all endpoints, ensuring real-time protection against malware and other security incidents.
- **Vulnerability Management**: superhack employs vulnerability management tools to proactively identify, assess, and remediate vulnerabilities across our internal systems and workplace devices.
- **Cloud Security Tools**: For cloud infrastructure, we rely on Cloud Security Posture Management (CSPM) and Cloud-Native Application Protection Platform (CNAPP) solutions to ensure the security and compliance of cloud environments. These tools provide real-time monitoring and automated compliance checks.

4.10 Adherence to Laws & Regulations

superhack is committed to complying with all relevant laws and regulations, ensuring that our operations and engagements align with legal and regulatory frameworks, particularly in areas concerning data protection and law enforcement:

- **GDPR Compliance**: In line with the EU General Data Protection Regulation (GDPR), superhack complies with data subject access requests (DSARs) where applicable. When acting as a data processor, we fully cooperate with our customers to ensure that data subject rights, such as the right to access, rectification, and erasure, are upheld.
- **Law Enforcement Cooperation**: superhack cooperates with law enforcement agencies when required to do so by law. However, all requests for data or access to systems are subject to careful legal review to ensure compliance with applicable regulations while protecting customer confidentiality and privacy.

---

5. Customer-Specific Customizations

superhack offers customization of TOMs for specific customer needs:

- **Custom Controls**: superhack can implement additional controls based on the customer's specific regulatory requirements.
- **Customer-Specific Incident Response**: Tailored incident response procedures can be established according to customer protocols.

---

6. Conclusion

superhack is committed to maintaining and continually improving its Technical and Organizational Measures. Regular reviews of this document ensure that superhack remains aligned with the latest security practices and regulatory requirements.