superhack

Data Processing

The Data Processing Agreement with its annexes, and the Transfer Impact Assessment.

1	Data Processing Agreement	Last updated 13.07.2026
2	Technical and Organizational Measures · DPA Annex I	Last updated 30.10.2026
3	Subprocessor List · DPA Annex II	Last updated 15.07.2026
4	Transfer Impact Assessment	

The Order Form is agreed separately with each customer. The current version of every document is published at superhack.app/legal.

Data Processing Agreement

Last updated 13.07.2026.

This Data Processing Agreement ("Agreement" or "DPA") is entered into between:

BLUE SKY SOFTWARE LTD, registered at Archiepiskopou Makariou III, 59, MOUYIAS TOWER,

6017, Larnaca, Cyprus ("Processor" or "superhack"), and the customer identified in the applicable Order Form ("Controller" or "Customer"),

Each a "Party" and collectively the "Parties".

This DPA forms part of and is subject to the Master Subscription Agreement ("MSA") between the Parties and reflects the Parties' agreement with respect to the processing of personal data by superhack on behalf of Customer.

---

1. Subject Matter and Purpose

The subject matter of this Agreement is the processing of personal data by superhack on behalf of Customer for the purpose of providing the superhack SaaS platform, which performs autonomous, AI-driven penetration testing against the Customer's authorized systems, applications, and infrastructure to identify security vulnerabilities and help the Customer remediate them.

---

2. Duration

This Agreement remains in effect for as long as superhack processes personal data on behalf of the Customer under the MSA.

---

3. Nature and Purpose of Processing

superhack processes personal data for the following purposes:

3.1 To provide and maintain the superhack SaaS platform and its features.

3.2 To perform security testing and to generate reports and findings on the Customer's authorized targets.

3.3 To provide support and communicate with the Customer.

3.4 To fulfill legal obligations and protect superhack's legitimate interests.

4. Categories of Data Subjects

- Authorized Users of the Customer's superhack account, and any individuals whose personal data may incidentally be present within the Customer's systems that are subject to authorized testing.

5. Categories of (Personal) Data Processed

This Agreement is provided to meet the requirements of the GDPR, which govern the processing of personal data. Beyond what the GDPR strictly requires, superhack also aims to be transparent about the categories of data it processes on behalf of the Customer. The following therefore documents the categories of personal data — and, where relevant, other data — that we may process in the course of delivering our services.

In the context of operating the superhack platform and delivering our services, personal data may arise from two fundamentally different sources: (i) data relating to the Customer's Authorized Users and their use of the platform, which is largely known and predictable; and (ii) data encountered within the Customer's own systems, applications, and services during authorized testing, the scope of which is determined solely by the Customer and is therefore not fully foreseeable by superhack. Specifically, we may process the following categories of data:

- **Identity and contact data** — names and email addresses of the Customer's Authorized Users.
- **Account and authentication data** — superhack platform usernames, login credentials, and authentication factors.
- **Access credentials provided for testing** — where the Customer provides credentials, API tokens, or keys so that superhack can test or scan systems, applications, or services in an authenticated state, we process these credentials as necessary to perform the authorized engagement.
- **Content and data encountered during testing** — when testing in an authenticated state, our agents may be exposed to any and all data — including personal data — present within the in-scope systems, applications, and services. The nature and extent of this data is determined solely by the Customer's decisions about which systems and what level of access to grant, and cannot be foreseen or exhaustively known by superhack in advance. For example, where the Customer grants access to code repositories, this may include the names and email addresses of the individuals who authored commits.
- **Activity and audit data** — logs indicating which Authorized Users initiated tests, configured scope, or accessed findings; sharing actions and permission changes involving personal accounts; and timestamps and contextual metadata for audit trails.
- **Device and technical metadata** — device type and identifiers such as browser and operating system used to access the platform.

Clarification: superhack does not seek to exfiltrate or retain personal data from the Customer's systems beyond what is necessary to evidence, reproduce, and remediate a finding. Where the

Customer provides credentials or API tokens to enable authenticated testing, these are processed solely for the purpose of performing the authorized testing.

6. Processing Instructions

superhack shall process personal data only in accordance with the documented instructions of the Customer, unless required to do otherwise by law. In such cases, superhack shall inform the Customer before processing unless prohibited by law.

7. Data Subject Rights

superhack shall, to the extent legally permitted, assist the Customer in fulfilling data subject requests under GDPR, including access, correction, erasure, and portability of personal data.

8. Subprocessors

8.1 Customer grants superhack a general written authorisation to engage subprocessors for the provision of the Services.

8.2 superhack will maintain an up-to-date list of subprocessors at Subprocessor List

8.3 Customer may object in writing, on reasonable data protection grounds, within thirty (30) days of such notification. The Parties will cooperate in good faith to implement a commercially reasonable alternative. If no such alternative is available, Customer's sole remedy shall be to discontinue use of the affected functionality. General termination rights under the MSA remain unaffected.

8.4 superhack will ensure that each subprocessor is bound by data protection obligations that are no less protective than those set out in this DPA.

9. International Transfers

9.1 superhack will primarily process personal data within the EEA. Where personal data is transferred to a country outside the EEA or to a country without an adequacy decision, superhack will ensure compliance with Chapter V GDPR, including by using Standard Contractual Clauses or other appropriate safeguards.

9.2 By entering into this DPA, Customer authorises such transfers insofar as they are necessary for the use of authorised subprocessors and the provision of the Services, subject to Customer's right to object to new or replacement subprocessors under Section 8.

10. Technical and Organisational Measures (TOMs)

superhack shall implement and maintain appropriate technical and organisational measures to protect personal data as required under Art. 32 GDPR. A description of these measures is available at Technical and Organizational Measures (TOM)

11. Data Breach Notification

In the event of a personal data breach, superhack shall notify the Customer without undue delay (≤ 48h from the time superhack becomes aware) and provide sufficient information to allow the Customer to meet any obligations to report or inform data subjects.

12. Data Deletion or Return

Upon termination of the MSA or upon written request, superhack shall delete or return all personal data to the Customer unless legal obligations require storage. superhack will confirm deletion in writing.

13. Confidentiality

superhack shall ensure that persons authorized to process the personal data are subject to confidentiality obligations.

14. Audits and Inspections

superhack shall make available information necessary to demonstrate compliance and allow for audits or inspections by the Customer or a mandated third party, subject to reasonable notice and frequency.

15. Liability and Indemnification

Each Party is liable for breaches of this Agreement in accordance with the liability clauses set out in the MSA.

16. Governing Law and Jurisdiction

This Agreement shall be governed by the laws of the Federal Republic of Germany. Venue shall be Berlin, Germany.

17. Annexes

The following annexes form an integral part of this Agreement and are incorporated by reference:

- **Annex I – Technical and Organisational Measures**: available at Technical and Organizational Measures (TOM)
- **Annex II – List of Subprocessors**: available at Subprocessor List

18. Miscellaneous

18.1 In case of conflict between the MSA and this DPA, the provisions of this DPA shall prevail with respect to the processing of personal data.

18.2 This DPA may be updated by mutual agreement in writing.

18.3 References to external documents (such as TOMs, Subprocessor List, and Annexes) are legally binding and form an integral part of this Agreement.

IN WITNESS WHEREOF, the Parties have caused this DPA to be executed by their authorized representatives.

Effective upon execution of the applicable Order Form referencing the superhack Master Subscription Agreement.

DPA Annex I

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.

DPA Annex II

Subprocessor List

Last updated 15.07.2026.

What is a Subprocessor?

At superhack, we use a small set of trusted third-party service providers to help us operate our platform reliably, securely, and at scale. Some of these partners process customer data in order to provide infrastructure, customer support, analytics, or product functionality. When they do so on our behalf, they qualify as **Subprocessors** under the GDPR. Each one is contractually bound by obligations that match or exceed those in our Data Processing Agreement (DPA).

Data Location and Safeguards for International Transfers

Most of our Subprocessor tenants are located in the European Union. Where a Subprocessor processes personal data outside the EEA, we rely on appropriate safeguards, such as the European Commission's Standard Contractual Clauses (SCCs), for the transfer.

In addition to SCCs, superhack performs a risk-based due diligence process before engaging any non-EEA Subprocessor. This includes:

- Direct engagement with the Subprocessor's security and data protection leadership (typically their CISO and/or DPO);
- A review of their technical and organizational measures (e.g. encryption practices, access control policies, audit reports);
- Alignment on contractual language that protects both superhack and its customers;
- Ongoing monitoring and periodic reassessments of their compliance posture.

This ensures we only work with vendors who meet our internal standards and customer expectations.

List of Third-Party Subprocessors

The table below lists our Subprocessors, the purpose for which each is engaged, the data it processes, whether it processes Customer data, and the region in which processing takes place.

Subprocessor	Purpose of Processing	Data Processed
Neon	Managed Postgres — the primary application database	Stores all tenant, asset, scan, finding, and user data

Render	Hosts the worker service that runs the scan agents	Processes target and scan data during authorized testing
Vercel	Hosts the web application; object storage via Vercel Blob	End-user data in transit; asset screenshots stored in Blob
Anthropic	Claude models via the Agent SDK — the core scan engine	Reads target and scan data to drive testing
OpenAI	CVE embeddings and small parsing calls	Reads target and scan data to drive testing
Resend	Transactional email delivery	Recipient email addresses and message content
PostHog	Product analytics (EU cloud)	Usage events, identifiers, IP addresses
Notion	Internal documentation and knowledge base	Business and operational data
Google Workspace	Email, calendar, and internal collaboration	Internal business communications
Slack	Internal team communication	Internal business communications
1Password	Credential and secret management	Internal access credentials and secrets

Changes to This List

This list may evolve as superhack grows. All changes will follow the notification process described above.

Transfer Impact Assessment

superhack – Transfer Impact Assessment (TIA) Information

This page provides information to assist superhack customers and partners in understanding how superhack handles data transfers to third countries, especially those outside the European Economic Area (EEA).

This page is provided for transparency and informational purposes only. It does not constitute a contractual commitment. For formal terms, please refer to our Data Processing Agreement (DPA)

Legal Background: Schrems II

In July 2020, the Court of Justice of the European Union (CJEU) invalidated the EU–U.S. Privacy Shield framework in the "Schrems II" ruling (C-311/18). The court confirmed that data transfers to third countries must be assessed for their adequacy under EU data protection standards. If the local legal framework falls short—particularly with regard to surveillance laws—data exporters are expected to implement additional safeguards to protect personal data.

This includes evaluating the impact of laws like:

- FISA 702 – which may allow U.S. intelligence agencies to request certain data from service providers.
- EO 12333 – which governs intelligence collection but does not independently authorize compelled data access.

How This Applies to superhack

superhack is operated by **BLUE SKY SOFTWARE LTD**, a Cyprus-based company with no legal presence in the United States. We do, however, use select U.S.-based subprocessors as part of delivering our service.

These providers may process limited amounts of personal data originating from the EEA. A full list of our subprocessors and their respective data transfer roles is available at: Subprocessor List

We rely on the European Commission's **Standard Contractual Clauses (SCCs)** for all data transfers outside the EEA and require all subprocessors to agree to equivalent protections through contractual terms.

AI Model Subprocessors

superhack uses third-party AI-model providers to power its testing agents and remains free to select and change these providers. Depending on the provider, some processing may take place outside the EEA (for example, in the United States). Where that is the case, we rely on appropriate safeguards, such as the European Commission's Standard Contractual Clauses, for the transfer.

superhack configures its use of these providers to be as privacy-protective as reasonably possible: to the fullest extent made available by each provider, we prevent them from using or retaining data or training their models on data submitted through the Services, and we minimize the personal data transmitted by filtering, redacting, or pseudonymizing it within our EU-based infrastructure before any model call.

Key Technical Safeguards

superhack has deployed a comprehensive range of technical security controls to secure our infrastructure, our platform, and the data we process on behalf of customers.

Critically, superhack minimizes the retention of sensitive data gathered from the Customer's systems during testing. Data captured as evidence of a finding is processed under strict access controls and is not retained beyond what is necessary to document, reproduce, and support remediation of the finding.

For a full overview of our technical and organizational security measures, please refer to our Technical and Organizational Measures (TOM).

Additional Measures

superhack is in the process of obtaining formal certifications under **SOC 2 Type II** and **ISO/IEC 27001**. In the meantime, we operate a fully aligned cyber & information security management system (CISMS) based on the requirements of both frameworks.

This includes:

- Documented security and risk management policies
- Regular internal audits
- Defined incident response procedures

Due Diligence on Subprocessors

While we do not conduct jurisdiction-specific legal assessments of each subprocessor, superhack performs vendor selection and ongoing monitoring based on:

- Publicly available information on security and compliance practices (e.g. whitepapers, certifications, audit reports)
- Contractual obligations under SCCs
- Alignment with our internal data protection standards

A current list of superhack's approved subprocessors is available here: Subprocessor List

---

Government Access Requests

As of the date below:

- superhack has **never received** a government request (including under FISA 702 or EO 12333) for access to customer data.
- In the event of any legally binding request, our policy is to:
  1. Notify the affected customer promptly (to the extent legally permitted)
  2. Limit disclosure strictly to what is legally required
  3. Challenge overbroad or unlawful demands where appropriate

---

Summary

Area	superhack Position
Legal Base for Transfers	Standard Contractual Clauses (SCCs)
Handling of Sensitive Data	Evidence minimized; captured only to document a finding and not retained beyond remediation needs
Certifications	In progress (SOC 2, ISO 27001); CISMS fully already operational
Government Requests	None received to date
Subprocessor Review	Contractual + risk-based due diligence

For further questions, contact us at: **legal@superhack.app**