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.