Transfer Impact Assessment

How international data transfers are assessed and safeguarded.

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**