HACKTHEBOX

Legal & Compliance: Data Security Measures

Effective: 01 August 2022

DATA SECURITY MEASURES

You should download a copy for future reference.

Where applicable, this will serve as the relevant Annex to the Standard Contractual Clauses and the DPA available at https://resources.hackthebox.com/hubfs/Legal/DPA.pdf. The following provides more information regarding HackTheBox's technical and organisational security measures.

Scope	Measures
Pseudonymization and encryption	HackTheBox maintains Subscriber Data in an encrypted format at rest using Advanced Encryption Standard and in transit using TLS.
Confidentiality, integrity, and availability and resilience of processing systems and services.	HackTheBox's service subscription agreements contain strict confidentiality obligations. Additionally, HackTheBox requires every downstream Subprocessor to sign confidentiality provisions that are substantially similar to those contained in HackTheBox's service subscription agreements. The infrastructure for the HackTheBox Services spans multiple fault-independent availability zones in geographic regions physically separated from one another, supported by various tools and processes to maintain high availability of services.
Restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident.	HackTheBox performs regular backups of Subscriber Data, which is hosted in the data centers. Backups are retained redundantly across multiple availability zones and encrypted in transit and at rest using Advanced Encryption Standard (AES-256).
Regular testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of processing.	HackTheBox maintains a risk-based assessment security program. The framework for HackTheBox's security program includes administrative, organisational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Subscriber Data. HackTheBox's security program is intended to be appropriate to the nature of the Services and the size and complexity of HackTheBox's business operations. HackTheBox has a separate and dedicated security team that manages HackTheBox's security program. This team facilitates and supports independent audits and assessments performed by third-parties to provide independent feedback on the operating effectiveness of the information security program.

User identification and authorization.	HackTheBox personnel are required to use unique user access credentials and passwords for authorization with enforced 2FA methods . HackTheBox follows the principles of least privilege through role-based and time-based access models when provisioning system access. HackTheBox personnel are authorized to access Subscriber Data based on their job function, role and responsibilities, and such access requires approval prior to access provisioning. Access is promptly removed upon role change or termination.
Protection of data during transmission.	Subscriber Data is encrypted when in transit between Subscriber and HackTheBox Services using TLS.
Protection of data during storage.	Subscriber Data is stored encrypted using the Advanced Encryption Standard.
Physical security of locations at which personal data are processed.	HackTheBox office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit televisions), and overall office security.
Event logging.	HackTheBox monitors access to applications, tools, and resources that process or store Subscriber Data, including cloud services. Monitoring of security logs is centralised by the security team. Log activities are investigated when necessary and escalated appropriately.
Systems configuration, including default configuration.	HackTheBox applies Secure Software Development Lifecycle (Secure SDLC) standards to perform numerous security-related activities for the Services across different phases of the product creation lifecycle from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before new Services are deployed; (b) annual penetration testing by independent third parties; and (c) threat models for new Services to detect any potential security threats and vulnerabilities. HackTheBox adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. Monitors are in place to notify the security team of changes made to critical infrastructure and services that do not adhere to the change management processes.

Internal IT and IT security governance and management.	HackTheBox maintains a risk-based assessment security program. The framework for HackTheBox's security program includes administrative, organisational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Subscriber Data. HackTheBox's security program is intended to be appropriate to the nature of the Services and the size and complexity of HackTheBox's business operations. HackTheBox has a separate and dedicated Information Security team that manages HackTheBox's security program. This team facilitates and supports independent audits and assessments performed by third parties. HackTheBox's security framework is based on the ISO 27001 Information Security Management System and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, and Security Monitoring and Incident Response. Security is managed at the highest levels of the company, with the Security Officer meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all HackTheBox employees for their reference.
Data minimization.	HackTheBox taking into account its legal obligations requires the minimum personal data in order to create an account and access and use the Service. Additionally, HackTheBox has built in self-service functionality to the Services that allow Subscribers to delete and update Subscriber Data.
Data quality.	HackTheBox has a three-fold approach for ensuring data quality. These measures include: (i) unit testing to ensure the quality of logic used to make API calls, (ii) volume testing to ensure the code is able to scale, and (iii) daily end-to-end testing to ensure that the input values match expected values. HackTheBox applies these measures across the board, both to ensure the quality of any Usage Data that HackTheBox collects and to ensure that the HackTheBox Platform is operating in accordance with the documentation. Each HackTheBox Subscriber chooses what Subscriber Data they route through the HackTheBox Services and how the Services are configured. As such, HackTheBox operates on a shared responsibility model. HackTheBox ensures that data quality is maintained from the time a Subscriber sends Subscriber Data into the Services and until that Subscriber Data leaves HackTheBox to flow to a downstream destination.

Limited data retention.	HackTheBox Subscribers unilaterally determine what Subscriber Data they route through the HackTheBox Services and how the Services are configured. As such, HackTheBox operates on a shared responsibility model. If a Subscriber is unable to delete Subscriber Data via the self-services functionality of the Services, then HackTheBox deletes Subscriber Data upon the Subscriber's written request, within the timeframe specified in the DPA and in accordance with applicable data protection law.
Accountability.	HackTheBox has adopted measures for ensuring accountability, such as implementing data protection policies across the business, maintaining documentation of processing activities, recording and reporting Security Incidents involving Personal Data, and appointing a Privacy and a Security Officer. Additionally, HackTheBox conducts regular third-party audits to ensure compliance with our privacy and security standards.
Data portability and erasure.	HackTheBox's Subscribers have direct relationships with their end users and are responsible for responding to requests from their end users who wish to exercise their rights under Applicable Data Protection Laws. HackTheBox has built-in self-service functionality to the Services that allow Subscribers to delete and modify Subscriber Data. If a Subscriber is unable to use such self-service functionality, HackTheBox specifies in the DPA that it will provide assistance to such Subscriber as may reasonably be require to comply with Subscriber's obligations under applicable data protection laws to respond to requests from individuals to exercise their rights under applicable data protection laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection). If HackTheBox receives a request from a Data Subject in relation to their Subscriber Data, HackTheBox will advise the Data Subject to submit their request to Subscriber, and Subscriber will be responsible for responding to any such request. When HackTheBox engages a sub-processor under, HackTheBox and the sub-processor shall enter into an agreement with data protection terms substantially similar to those contained herein. Each sub-processor agreement must ensure that HackTheBox is able to meet its obligations to Subscriber. In addition to implementing technical and organisational measures to protect personal data, sub-processors must a) notify HackTheBox in the event of a Security Incident so HackTheBox may notify Subscriber according to applicable law; b) delete data when instructed by HackTheBox in accordance with Subscriber's instructions to HackTheBox; c) not engage additional sub-processors without authorization; d) not change the location where data is processed; or e) process data in a manner which conflicts with Subscriber's instructions to HackTheBox.

HACKTHEBOX