Preview

GENERAL INFORMATION

edit

100%

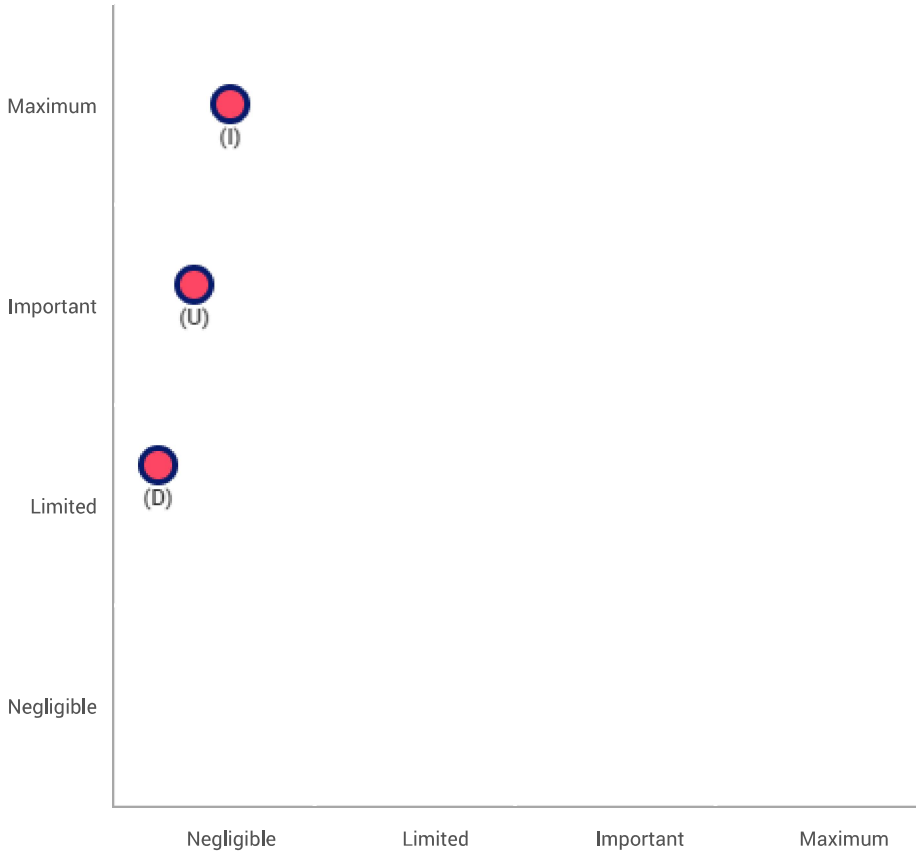
Preview

Editing :	Bipin, Adhikari	**Status :**	Simple validation
Evaluation :	Shubhika, Garg		
Validation :	Mayank, Narang		

Validation

Risk mapping

Risk seriousness



- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

10/27/23

Validation

Action plan

Overview

Fundamental principles

Purposes
Legal basis
Adequate data
Data accuracy
Storage duration
Information for the data subjects
Obtaining consent
Right of access and to data portability
Right to rectification and erasure
Right to restriction and to object
Subcontracting
Transfers

Planned or existing measures

Encryption
Traceability (logging)
Minimising the amount of personal data
Website security
Managing privacy risks
Physical access control

Risks

Illegitimate access to data
Unwanted modification of data
Data disappearance

Improvable Measures
Acceptable Measures

Fundamental principles

No action plan recorded.

Existing or planned measures

No action plan recorded.

Risks

No action plan recorded.

Validation

TO TRANSLATE - DPO and data subjects opinion

DPO's name

Adhikari, Garg, Narang

DPO's status

The treatment could be implemented.

DPO's opinion

Most of the security risks have been mitigated by the platform itself, so we did not find any major or

minor improvements to suggest. Moreover, legal and complicance information are properly documented already.

Search of concerned people opinion

Concerned people opinion wasn't requested.

Reason why concerned people opinion wasn't requested

Within our social circles we were not able to find users who were concerned for their privacy while using HackTheBox.

Context

Overview

What is the processing under consideration?

The processing under consideration is the treatment of personal data by HackTheBox through their online service, which can be found at www.hackthebox.com.

What are the responsibilities linked to the processing?

The responsibilities linked to the processing include: safeguarding user data, ensuring the accuracy and legality of the data, obtaining necessary consents and data retention for as long as necessary to fulfill its purposes. According to its policy, HackTheBox is not obligated to investigate the details of Subscriber instructions or Personal Data beyond legal requirements.

Are there standards applicable to the processing?

The standards applicable to the processing are those defined by: GDPR, applicable national laws, regulation and guidelines from the competent data protection authority, any applicable successor texts or other similar national data protection laws and Standard Contractual Clauses approved by the European Commission in case of information sent outside of the European Economic Area.

Evaluation : Acceptable

Context

Data, processes and supporting assets

What are the data processed?

The data processed includes: information that certifies the user identity (e.g., name, address, credit card details...), account information, information about payment methods, history of contact with HackTheBox and any other information provided by the user (e.g., in case of breaches of their Acceptable Use Policy).

How does the life cycle of data and processes work?

Data is collected by HackTheBox starting from the registration phase and it is retained for as long as necessary to fulfill the purposes of satisfying any legal, accounting or reporting requirements. The service determines the appropriate retention period by considering the volume, nature and sensitivity of the personal data as well as the potential risk of harm. Moreover, as per their Data Protection Addendum, personal data may be retained for up to two years following the end of the Subscriber Agreement.

What are the data supporting assets?

An asset provided by HackTheBox to support data retention is the "Vault", i.e. an AES-encrypted and passphrase-protected storage which adds a layer of protection to personal data. Moreover, on its website, a list can be found of the specific processors and subprocessors linked to this service.

Examples of processors include PAYPAL (for billing in the EU), Snowflake (for reporting functionality in the USA) and Leaseweb UK Limited (for hosting purposes in the UK). Examples of subprocessors include XERO (for billing and accounting in the USA), Hetzner Online GmbH (for hosting purposes in the EU) and AMITO LTD (for hosting purposes in the UK).

Regular backups of user data are made in their data centers.

Evaluation : Acceptable
Evaluation comment :
The data retention period is two years.

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

The processing purposes are indeed specified explicitly on the HackTheBox website for purposes of transparency as well as compliance with legal obligations.

Evaluation : Acceptable

What are the legal basis making the processing lawful?

The legal basis include: to enter into and perform Subscriber Agreements, to comply with legal obligations, to pursue legitimate interests (if not outweighted by the Subscriber's rights and freedoms), for purposes the Subscriber gave clear and unconditional consent for.

Evaluation : Acceptable

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

The data collected indeed seems to be limited to the necessary informations for account creation and usage of the service.

Evaluation : Acceptable

Are the data accurate and kept up to date?

According to HackTheBox's Privacy Notice, measures are enforced to make sure data is always accurate and up to date.

Evaluation : Acceptable

What are the storage duration of the data?

Data is stored for up to two years following the end of the Subscriber Agreement.

Evaluation : Acceptable
Evaluation comment :
Typo: it is actually two years.

Fundamental principles

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

HackTheBox's Subscribers have direct relationships with their end users and are responsible for responsing to requests from their end users who wish to exercise their rights under Applicable Data Protection Laws.

Evaluation : Acceptable

If applicable, how is the consent of data subjects obtained?

When first accessing the service's website, users are presented with all the necessary information regarding data collection as well as with the possibility to opt-out from all or some of this processings.

Moreover, during the subscription procedure, users have to agree to Terms of Service and Privacy Policy in order to finalize their account creation.

Evaluation : Acceptable

How can data subjects exercise their rights of access and to data portability?

HackTheBox contains built-in functionalities to allow Subscribers to exercise their rights of access and data potability. If a Subscriber is unable to use such self-service functionalities, HackTheBox will provide assistance as may reasonably by required to complice with contractual obligations.

Evaluation : Acceptable

How can data subjects exercise their rights to rectification and erasure?

HackTheBox has some built-in functionalities to allow users to exercise their rights to rectification and erasure. If a user is unable to use such self-service functionalities, HackTheBox will provide assistance as may reasonably by required to complice with contractual obligations.

Evaluation : Acceptable

How can data subjects exercise their rights to restriction and to object?

HackTheBox has some built-in functionalities to allow users to exercise their rights to restriction and to object. If a Subscriber is unable to use those self-service functionalities, HackTheBox will provide assistance as may reasonably by required to complice with contractual obligations.

Evaluation : Acceptable

Are the obligations of the processors clearly identified and governed by a contract?

Users stipulate a Subscriber Agreement with HackTheBox during the creation of their account on the

service.

Evaluation : Acceptable

In the case of data transfer outside the European Union, are the data adequately protected?

As per HackTheBox's Privacy Notice, in case of data transfer outside of the European Economic Area or the UK, such information receives a certain level of protection by only sending information to countries that have been formally recognized and approved by the European Commission or using Standard Contractual Clauses approved by the European Commission.

Evaluation : Acceptable

Risks

Planned or existing measures

Encryption

Data Confidentiality is ensured using the Advanced Encryption Standard (AES) and, in transit, using Transport Layer Security (TLS).

Evaluation : Acceptable

Traceability (logging)

HackTheBox monitors access to applications, tools and resources that process or store Subscriber Data, including cloud services. Events are logged for as long as deemed necessary for purposes such as investigations

Evaluation : Acceptable

Minimising the amount of personal data

Legal obligations indicated on the service's Data Security Measures require HackTheBox to only collect the minimum personal data in order to create an account and access and use the service.

Evaluation : Acceptable

Website security

Controls implemented for website security include SSH and TLS.

Evaluation : Acceptable

Managing privacy risks

HackTheBox performs activities to manage and control privacy risks. These include internal security reviews before new Services are deployed, annual penetration testing by independent third parties, threat models for new Service to detect any potential security threats and vulnerabilities.

Evaluation : Acceptable

Physical access control

HackTheBox office spaces have a physical security program that manages visitors, building entrances, CCTVs and overall office security.

Evaluation : Acceptable

Risks

Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?

Financial fraud., Identity Theft., Loss of Trust.

What are the main threats that could lead to the risk?

Cyberattacks, Insider Threats, Natural disasters

What are the risk sources?

Insecure APIs., Weak authentication services, Employers with access to the data

Which of the identified planned controls contribute to addressing the risk?

Encryption, Physical access control, Minimising the amount of personal data, Website security

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Maximum, The HackTheBox website deals with important private data such as credit card or ID information, so the impact of potential hackers acquiring it would be huge.

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, If users follow ethical guidelines, the likelihood of the risk is relatively low.

Evaluation : Acceptable

Risks

Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?

Identity Theft., Financial fraud., Data accuracy

What are the main threats that could lead to the risk?

Cyberattacks, Social Engineering, Insider Threats

What are the risk sources?

Weak access control, Physical access vulnerabilities, Third-party vendors

Which of the identified controls contribute to addressing the risk?

Website security, Physical access control, Traceability (logging), Encryption

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, The impact of these risks being exploited would be significant.

How do you estimate the likelihood of the risk, especially in respect of threats, sources

Risks

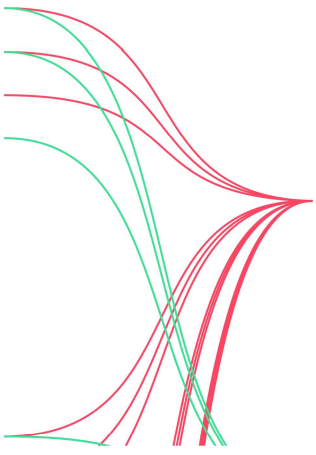
Risks overview

Potential impacts

- Financial fraud.
- Identity Theft.
- Loss of Trust.
- Data accuracy
- Financial damage
- Loss of progress
- Reputational damage

Threats

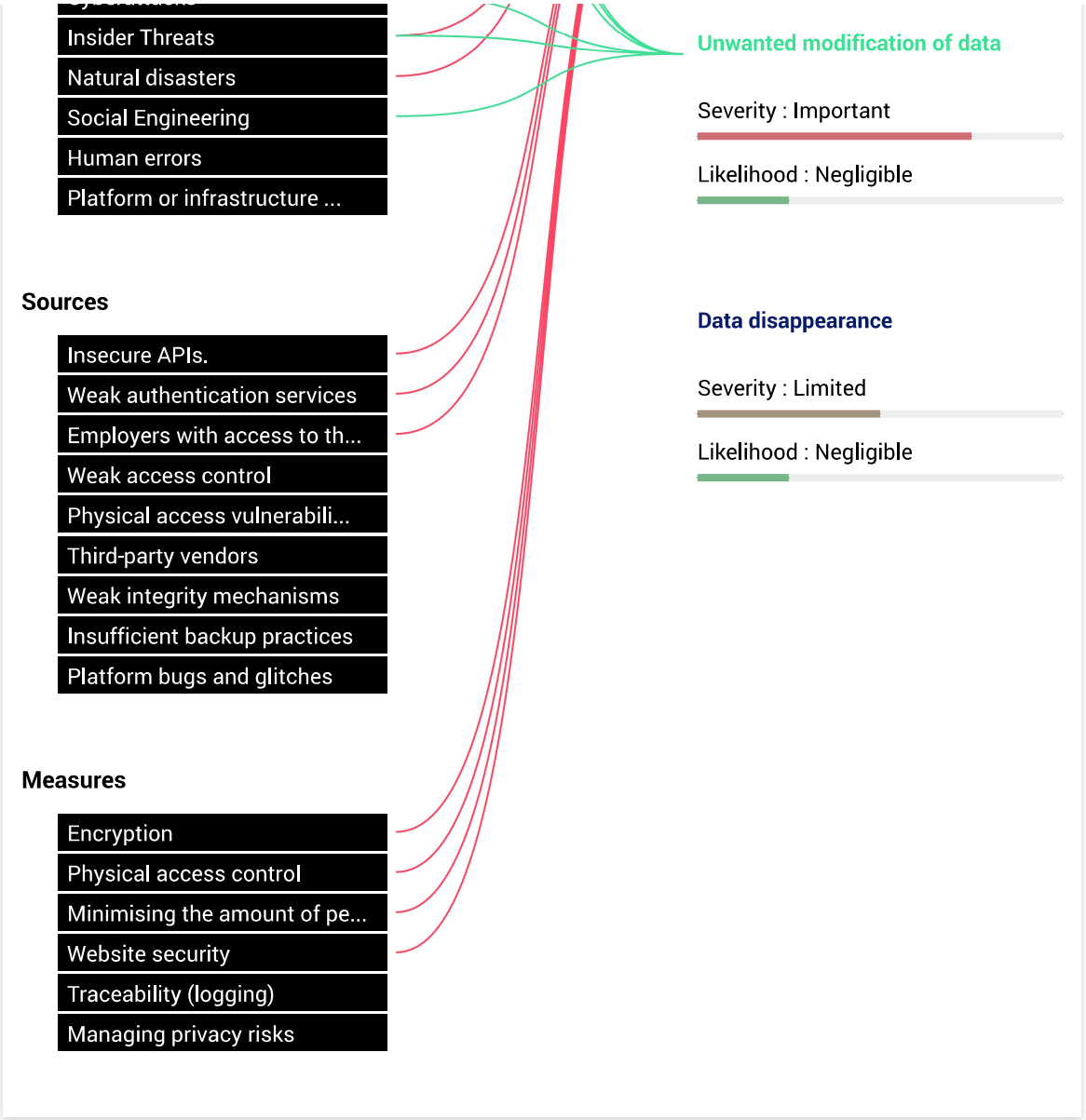
- Cyberattacks



Illegitimate access to data

Severity : Maximal

Likelihood : Negligible


Insider Threats
Natural disasters
Social Engineering
Human errors
Platform or infrastructure ...
Sources
Insecure APIs.
Weak authentication services
Employers with access to th...
Weak access control
Physical access vulnerabili...
Third-party vendors
Weak integrity mechanisms
Insufficient backup practices
Platform bugs and glitches
Measures
Encryption
Physical access control
Minimising the amount of pe...
Website security
Traceability (logging)
Managing privacy risks
Unwanted modification of data
Severity : Important
Likelihood : Negligible
Data disappearance
Severity : Limited
Likelihood : Negligible