GDPR Gap Assessment from Vanta

FOR TERRA

GDPR is a privacy regulation that requires businesses to protect the personal data and privacy of EU citizens. It affects all companies that do business or have employees in the EU. This gap analysis maps Terra's compliance controls to the GDPR framework. This gap analysis can:

- provide an illustrative set of controls appropriate to demonstrate your GDPR framework
- identify control gaps
- give advice on ways to satisfy the unimplemented controls.

The table to the right presents a summary of the gap analysis; the implemented controls are shown as such, while the unimplemented controls are broken down by their severity, which can be used to prioritize fixes.

Chapter 2

Principles

Article 6

Lawfulness of processing

2 CONTROLS

Identify lawful basis

✓ COMPLETE

The company documents the lawful basis for PII processing.

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Identity and document purpose

✓ COMPLETE

The company documents the purpose for which PII is processed.

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Article 7

Conditions for consent

3 CONTROLS

Consent obtained

✓ COMPLETE

The company determines and documents when and how consent was obtained.

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Modify or withdraw consent

✓ COMPLETE

The company provides a mechanism to modify or withdraw consent.

Guidance: This is typically the data subject access request process.

2 DOCUMENTS

Cookie consent manager ✓

Publicly available privacy policy ✓

Object to PII processing

✓ COMPLETE

The company provides a mechanism for data subjects to object to processing.

Guidance: This is typically the data subject access request process.

1 DOCUMENT

Publicly available privacy policy ✓

Chapter 3

Rights of the data subject

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

2 CONTROLS

Handling DSAR requests

✓ COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

PII data subject notice

✓ COMPLETE

The company determines and documents requirements for notice to data subjects and the timing of the notice.

1 DOCUMENT

Maintain data inventory map ✓

Article 13

Information to be provided where personal data are collected from the data subject

3 CONTROLS

Handling DSAR requests

✓ COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

PII data subject information

✓ COMPLETE

The company provides data subjects clear and easily accessible information identifying the controller and describing the PII processing.

2 DOCUMENTS

Cookie Policy ✓

Publicly available privacy policy ✓

PII data subject notice

✓ COMPLETE

The company determines and documents requirements for notice to data subjects and the timing of the notice.

1 DOCUMENT

Maintain data inventory map ✓

Article 14

Information to be provided where personal data have not been obtained from the data subject

2 CONTROLS

Handling DSAR requests

✓ COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

PII data subject notice

✓ COMPLETE

The company determines and documents requirements for notice to data subjects and the timing of the notice.

1 DOCUMENT

Maintain data inventory map ✓

Article 15

Right of access by the data subject

3 CONTROLS

Access, correction and/or erasure

✓ COMPLETE

Defined process and procedure for data subjects to access and correct their PII.

Guidance: This is typically the data subject access request process.

1 DOCUMENT

Publicly available privacy policy ✓

Copy of PII processed

COMPLETE

Establish a process of providing a copy of PII to data subjects upon verified request.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Handling DSAR requests

COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Article 16

Right to rectification

2 CONTROLS

Access, correction and/or erasure

COMPLETE

Defined process and procedure for data subjects to access and correct their PII.

Guidance: This is typically the data subject access request process.

1 DOCUMENT

Publicly available privacy policy

Handling DSAR requests

COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Article 17

Right to erasure (‘right to be forgotten’)

1 CONTROL

Handling DSAR requests

COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Article 18

Right to restriction of processing

1 CONTROL

Handling DSAR requests

✓ COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

2 CONTROLS

Handling DSAR requests

✓ COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

PII controllers' obligations to inform third parties

COMPLETE

Establish a process, policies and procedures for notifying sub processors of corrections, deletions or withdrawals of PII.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Article 20

Right to data portability

1 CONTROL

Handling DSAR requests

COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Article 21

Right to object

2 CONTROLS

Automated decision making

✓ COMPLETE

Identify and address obligations to data subjects resulting from decisions made from automated processing (if applicable).

1 DOCUMENT

Data Protection Impact Assessment (DPIA) ✓

Handling DSAR requests

✓ COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

Article 22

Automated individual decision-making, including profiling

2 CONTROLS

Automated decision making

✓ COMPLETE

Identify and address obligations to data subjects resulting from decisions made from automated processing (if applicable).

1 DOCUMENT

Data Protection Impact Assessment (DPIA) ✓

Handling DSAR requests

✓ COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

Article 23

Restrictions

1 CONTROL

Handling DSAR requests

✓ COMPLETE

Define and document procedures for handling Data Subject Access Requests (DSAR).

Vanta has a partnership with Transcend to assist with Handling DSAR requests at a discounted pricing for our customers.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

Chapter 4

Controller and Processor

Article 24

Responsibility of the controller

31 CONTROLS

Access requests required

COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

4 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta.

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta.

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy.

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities.

Access reviews conducted

COMPLETE

The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

1 DOCUMENT

Proof of completed access review

Access revoked upon termination

COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

2 DOCUMENTS

Employee termination checklist

Employee termination security policy

Accuracy and quality

COMPLETE

The company has a process to ensure that PII is complete, accurate, and up-to-date.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Anti-malware technology utilized

COMPLETE

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

1 TEST

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed.

Asset disposal procedures utilized

COMPLETE

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

1 DOCUMENT

Proof of media/device disposal

Continuity and Disaster Recovery plans established

COMPLETE

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.

1 DOCUMENT

Tabletop disaster recovery exercise

Continuity and Disaster Recovery plans tested annually

✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Data classification policy established

✓ COMPLETE

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

Data encryption utilized

✓ COMPLETE

The company's datastores housing sensitive customer data are encrypted at rest.

2 TESTS

User data is encrypted at rest: Verifies that all Amazon RDS instances are encrypted. ✓

User data in S3 is encrypted at rest (AWS): Verifies that all AWS S3 buckets marked as containing user data are encrypted. ✓

Data transmission encrypted

✓ COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

GDPR training is implemented

✓ COMPLETE

The company requires employees to complete GDPR awareness training within thirty days of hire and annually thereafter.

2 TESTS

GDPR security awareness training selected: Verifies that a GDPR security awareness training program has been selected within Vanta. ✓

GDPR security awareness training records tracked: Verifies that all relevant employees have uploaded documentation indicating that they have completed GDPR security training. ✓

Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

1 TEST

CloudTrail enabled: Verifies that all linked AWS accounts have CloudTrail enabled. ✓

MDM system utilized

✓ COMPLETE

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

1 TEST

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed. ✓

Network and system hardening standards maintained

✓ COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

5 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Network firewalls reviewed

✓ COMPLETE

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.

2 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Network firewalls utilized

✓ COMPLETE

The company uses firewalls and configures them to prevent unauthorized access.

2 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Network segmentation implemented

✓ COMPLETE

The company's network is segmented to prevent unauthorized access to customer data.

1 DOCUMENT

Network segregation ✓

Password policy enforced

✓ COMPLETE

The company requires passwords for in-scope system components to be configured according to the company's policy.

1 TEST

Password policy configured for infrastructure: Verifies that all AWS accounts have password policies enabled. ✓

PII transmission controls for controller

✓ COMPLETE

The company implements technical controls to ensure data transmitted to third parties reaches its destination.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

PII transmission controls for processor

✓ COMPLETE

The company encrypts PII in transit.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

Portable media encrypted

COMPLETE

The company encrypts portable and removable media devices when used.

1 TEST

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta.

1 DOCUMENT

Removable media encryption

Production deployment access restricted

COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

4 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta.

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta.

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch for all linked version control repositories.

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days.

Production inventory maintained

COMPLETE

The company maintains a formal inventory of production system assets.

3 TESTS

Inventory items have descriptions: Verifies that all items on the Vanta inventory page have descriptions.

Inventory items have owners: Verifies that all items on the Vanta inventory page have been assigned owners.

Inventory list tracks resources that contain user data: Verifies that these resource types - storage buckets, databases, PaaS apps, queues, data warehouses, or custom items - are marked as containing user data in Vanta.

Production network access restricted

COMPLETE

The company restricts privileged access to the production network to authorized users with a business need.

1 TEST

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta.

Remote access encrypted enforced

COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

1 TEST

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

Remote access MFA enforced

COMPLETE

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.

3 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human.

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled.

MFA on infrastructure root accounts (AWS): Verifies that all AWS root accounts have MFA enabled.

Service infrastructure maintained

COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

4 TESTS

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker.

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker.

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag.

Records of security issues being closed within SLA: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag are resolved within the SLA set in Vanta.

2 DOCUMENTS

Sample of remediated vulnerabilities

Vulnerability scan

Unique account authentication enforced

COMPLETE

The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.

7 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached.

Employees have unique email accounts: Verifies that every linked identity provider has more than one user.

Employees have unique infrastructure accounts: Verifies that every linked AWS and Heroku account have at least one user.

Employees have unique version control accounts: Verifies that every linked version control account has more than one user.

Service accounts used: Verifies that every AWS account is assigned a role.

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days.

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users.

Unique network system authentication enforced

COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

1 TEST

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

Article 25

Data protection by design and by default

8 CONTROLS

Customer data deleted upon leave

COMPLETE

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

1 TEST

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta.

1 DOCUMENT

Customer data deletion record

Data classification policy established

COMPLETE

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta.

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy.

Disposal of PII

COMPLETE

The company documents policies, procedures and mechanism for disposal of PII.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta.

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy.

Limit collection

COMPLETE

The company limits collection of PII to the minimum that is necessary for it's purposes.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

PII de-identification and deletion at the end of processing

COMPLETE

The company deletes or de-identifies when no longer needed.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta.

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy.

1 DOCUMENT

Customer data deletion record

PII minimization

COMPLETE

The company ensures that it only collects and processes data which it needs for its purposes.

1 DOCUMENT

Maintain data inventory map

Retention of PII

✓ COMPLETE

The company does not retain PII longer than necessary for its purposes.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

1 DOCUMENT

Customer data deletion record ✓

Return, transfer or disposal of PII

✓ COMPLETE

The company returns, transfers, disposes PII in accordance to its policies and commitments. (SCC 8.5)

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

2 DOCUMENTS

Customer data deletion record ✓

Data Processing Agreements (DPA) with customers ✓

Article 27

Representatives of controllers or processors not established in the Union

1 CONTROL

Appoint EU representative

✓ COMPLETE

The company shall appoint an EU based representative.

1 DOCUMENT

EU representative appointed ✓

Article 28

Processor

38 CONTROLS

Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

4 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Access reviews conducted

✓ COMPLETE

The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

1 DOCUMENT

Proof of completed access review ✓

Access revoked upon termination

✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

2 DOCUMENTS

Employee termination checklist ✓

Employee termination security policy ✓

Anti-malware technology utilized

✓ COMPLETE

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

1 TEST

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed. ✓

Asset disposal procedures utilized

✓ COMPLETE

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

1 DOCUMENT

Proof of media/device disposal ✓

Assist controllers with privacy obligations

✓ COMPLETE

The company's Data Processing Agreements (DPA) with the customers (controllers) commit to assisting them with privacy obligations.

1 DOCUMENT

Data Processing Agreements (DPA) with customers ✓

Basis for PII transfer between jurisdictions

✓ COMPLETE

The company's Master Services Agreement (MSA) informs the customer of the legal basis for transfers between jurisdictions and allows customers to object to changes or terminate service.

1 DOCUMENT

Data Processing Agreements (DPA) with customers ✓

Continuity and Disaster Recovery plans established

✓ COMPLETE

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Continuity and Disaster Recovery plans tested annually

✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Customer obligations

✓ COMPLETE

The company provides their customer with information sufficient for them to demonstrate their privacy compliance. (SCC 8.9(b))

1 DOCUMENT

Data Processing Agreements (DPA) with customers ✓

Data classification policy established

✓ COMPLETE

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

Data encryption utilized

✓ COMPLETE

The company's datastores housing sensitive customer data are encrypted at rest.

2 TESTS

User data is encrypted at rest: Verifies that all Amazon RDS instances are encrypted. ✓

User data in S3 is encrypted at rest (AWS): Verifies that all AWS S3 buckets marked as containing user data are encrypted. ✓

Data transmission encrypted

✓ COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

Disclosure of subcontractors used to process PII

✓ COMPLETE

The company discloses all PII sub processors to the customer.

1 TEST

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

1 DOCUMENT

Data Processing Agreements (DPA) with customers ✓

GDPR training is implemented

✓ COMPLETE

The company requires employees to complete GDPR awareness training within thirty days of hire and annually thereafter.

2 TESTS

GDPR security awareness training selected: Verifies that a GDPR security awareness training program has been selected within Vanta. ✓

GDPR security awareness training records tracked: Verifies that all relevant employees have uploaded documentation indicating that they have completed GDPR security training. ✓

Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

Infringing instruction

✓ COMPLETE

The company informs the customer if processing instructions are illegal. (SCC 8.1(b))

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

1 TEST

CloudTrail enabled: Verifies that all linked AWS accounts have CloudTrail enabled. ✓

Marketing and advertising use

COMPLETE

The company does not use the PII collected for services for marketing and advertising without consent.

Consent for marketing is not required for using services.

1 DOCUMENT

Data Processing Agreements (DPA) with customers

MDM system utilized

COMPLETE

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

1 TEST

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed.

Network and system hardening standards maintained

COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

5 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta.

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy.

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached.

Firewall default disallows traffic: This feature is built into AWS.

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta.

Network firewalls reviewed

✓ COMPLETE

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.

2 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Network firewalls utilized

✓ COMPLETE

The company uses firewalls and configures them to prevent unauthorized access.

2 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Network segmentation implemented

✓ COMPLETE

The company's network is segmented to prevent unauthorized access to customer data.

1 DOCUMENT

Network segregation ✓

Password policy enforced

✓ COMPLETE

The company requires passwords for in-scope system components to be configured according to the company's policy.

1 TEST

Password policy configured for infrastructure: Verifies that all AWS accounts have password policies enabled. ✓

PII transmission controls for controller

✓ COMPLETE

The company implements technical controls to ensure data transmitted to third parties reaches its destination.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

PII transmission controls for processor

✓ COMPLETE

The company encrypts PII in transit.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

Portable media encrypted

✓ COMPLETE

The company encrypts portable and removable media devices when used.

1 TEST

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

1 DOCUMENT

Removable media encryption ✓

Process as per processor agreements

✓ COMPLETE

The company only processes PII for the purposes expressed in contract (SCCs 8.1 and 8.2).

2 DOCUMENTS

Data Processing Agreements (DPA) with customers ✓

Maintain data inventory map ✓

Production deployment access restricted

✓ COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

4 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch for all linked version control repositories. ✓

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days. ✓

Production inventory maintained

✓ COMPLETE

The company maintains a formal inventory of production system assets.

3 TESTS

Inventory items have descriptions: Verifies that all items on the Vanta inventory page have descriptions. ✓

Inventory items have owners: Verifies that all items on the Vanta inventory page have been assigned owners. ✓

Inventory list tracks resources that contain user data: Verifies that these resource types - storage buckets, databases, PaaS apps, queues, data warehouses, or custom items - are marked as containing user data in Vanta. ✓

Production network access restricted

COMPLETE

The company restricts privileged access to the production network to authorized users with a business need.

1 TEST

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta.

Remote access encrypted enforced

COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

1 TEST

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

Remote access MFA enforced

COMPLETE

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.

3 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human.

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled.

MFA on infrastructure root accounts (AWS): Verifies that all AWS root accounts have MFA enabled.

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

4 TESTS

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

Records of security issues being closed within SLA: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag are resolved within the SLA set in Vanta. ✓

2 DOCUMENTS

Sample of remediated vulnerabilities ✓

Vulnerability scan ✓

Sub-processor changes

✓ COMPLETE

The company communicates the changes to sub-processors to the customer in writing with the opportunity to object.

3 DOCUMENTS

Data Processing Agreements (DPA) with customers ✓

MSA template ✓

Sub-processor change communication plan ✓

Unique account authentication enforced

COMPLETE

The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.

7 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached.

Employees have unique email accounts: Verifies that every linked identity provider has more than one user.

Employees have unique infrastructure accounts: Verifies that every linked AWS and Heroku account have at least one user.

Employees have unique version control accounts: Verifies that every linked version control account has more than one user.

Service accounts used: Verifies that every AWS account is assigned a role.

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days.

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users.

Unique network system authentication enforced

COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

1 TEST

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

Article 30

Records of processing activities

8 CONTROLS

Countries and international organizations to which PII can be stored for processor

✓ COMPLETE

The company documents all countries where PII is stored.

1 DOCUMENT

Maintain data inventory map ✓

Countries and international organizations to which PII can be transferred for controller

✓ COMPLETE

The company specifies and documents the countries and international organizations where PII is transferred.

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Data inventory

✓ COMPLETE

The company creates and maintains a PII data inventory.

For controllers:

- the name and contact details of the controller
- the purpose behind the processing of data
- a description of the categories of data that will be processed
- who will receive the data including data
- documentation of suitable safeguards for data transfers to a third country or an international organization
- the retention period of the different categories of data
- a general description of the technical and organizational security measures

For processors:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer
- the categories of processing carried out on behalf of each controller
- documentation of suitable safeguards for data transfers to a third country or an international organization
- a general description of the technical and organizational security measures

1 DOCUMENT

Maintain data inventory map ✓

Identify basis for PII transfer between jurisdictions

✓ COMPLETE

The company identifies and documents its legal basis for transferring between jurisdictions.

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Notification of PII disclosure requests

✓ COMPLETE

The company communicates legally binding disclosures for PII to the customer before disclosure where possible. (SCC 15.1-2)

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

1 DOCUMENT

Data Processing Agreements (DPA) with customers ✓

Records of PII disclosure to third parties

✓ COMPLETE

The company should record disclosure of PII to third parties including what has been disclosed and what time.

1 DOCUMENT

Maintain data inventory map ✓

Records of transfer of PII

✓ COMPLETE

The company documents transfers of PII to or from third parties and ensures cooperation with the requests from data subjects.

2 DOCUMENTS

Data Processing Agreements (DPA) with customers ✓

Maintain data inventory map ✓

Records related to processing PII

✓ COMPLETE

The company maintains necessary privacy records.

1 DOCUMENT

Maintain data inventory map ✓

Article 32

Security of processing

31 CONTROLS

Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

4 TESTS

Company has an approved Access Control Policy: Verifies that a Access Control Policy has been created and approved within Vanta. ✓

Company has an approved Information Security Roles and Responsibilities: Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

Employees agree to Access Control Policy: Verifies that all relevant employees have agreed to the Access Control Policy. ✓

Employees agree to Information Security Roles and Responsibilities: Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓

Access reviews conducted

✓ COMPLETE

The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

1 DOCUMENT

Proof of completed access review ✓

Access revoked upon termination

COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

2 DOCUMENTS

Employee termination checklist

Employee termination security policy

Accuracy and quality

COMPLETE

The company has a process to ensure that PII is complete, accurate, and up-to-date.

2 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Anti-malware technology utilized

COMPLETE

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

1 TEST

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed.

Asset disposal procedures utilized

COMPLETE

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

1 DOCUMENT

Proof of media/device disposal

Continuity and Disaster Recovery plans established

✓ COMPLETE

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Continuity and Disaster Recovery plans tested annually

✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Data classification policy established

✓ COMPLETE

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

2 TESTS

Company has an approved Data Management Policy: Verifies that a Data Management Policy has been created and approved within Vanta. ✓

Employees agree to Data Management Policy: Verifies that all relevant employees have agreed to the Data Management Policy. ✓

Data encryption utilized

✓ COMPLETE

The company's datastores housing sensitive customer data are encrypted at rest.

2 TESTS

User data is encrypted at rest: Verifies that all Amazon RDS instances are encrypted. ✓

User data in S3 is encrypted at rest (AWS): Verifies that all AWS S3 buckets marked as containing user data are encrypted. ✓

Data transmission encrypted

✓ COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

1 TEST

CloudTrail enabled: Verifies that all linked AWS accounts have CloudTrail enabled. ✓

MDM system utilized

✓ COMPLETE

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

1 TEST

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed. ✓

Network and system hardening standards maintained

✓ COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

5 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Network firewalls reviewed

✓ COMPLETE

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.

2 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Network firewalls utilized

✓ COMPLETE

The company uses firewalls and configures them to prevent unauthorized access.

2 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Network segmentation implemented

✓ COMPLETE

The company's network is segmented to prevent unauthorized access to customer data.

1 DOCUMENT

Network segregation ✓

Password policy enforced

✓ COMPLETE

The company requires passwords for in-scope system components to be configured according to the company's policy.

1 TEST

Password policy configured for infrastructure: Verifies that all AWS accounts have password policies enabled. ✓

PII transmission controls for controller

✓ COMPLETE

The company implements technical controls to ensure data transmitted to third parties reaches its destination.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

PII transmission controls for processor

✓ COMPLETE

The company encrypts PII in transit.

4 TESTS

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

Portable media encrypted

COMPLETE

The company encrypts portable and removable media devices when used.

1 TEST

Company has an approved Cryptography Policy: Verifies that a Cryptography Policy has been created and approved within Vanta.

1 DOCUMENT

Removable media encryption

Production deployment access restricted

COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

4 TESTS

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta.

Company has an approved Secure Development Policy: Verifies that a Secure Development Policy has been created and approved within Vanta.

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch for all linked version control repositories.

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days.

Production inventory maintained

COMPLETE

The company maintains a formal inventory of production system assets.

3 TESTS

Inventory items have descriptions: Verifies that all items on the Vanta inventory page have descriptions.

Inventory items have owners: Verifies that all items on the Vanta inventory page have been assigned owners.

Inventory list tracks resources that contain user data: Verifies that these resource types - storage buckets, databases, PaaS apps, queues, data warehouses, or custom items - are marked as containing user data in Vanta.

Production network access restricted

COMPLETE

The company restricts privileged access to the production network to authorized users with a business need.

1 TEST

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta.

Pseudonymization

COMPLETE

The company determines any need for pseudonymization and implement it as needed.

2 DOCUMENTS

Data Protection Impact Assessment (DPIA)

Pseudonymization procedure implemented

Remote access encrypted enforced

COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

1 TEST

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

Remote access MFA enforced

COMPLETE

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.

3 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human.

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled.

MFA on infrastructure root accounts (AWS): Verifies that all AWS root accounts have MFA enabled.

Service infrastructure maintained

COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

4 TESTS

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker.

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker.

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag.

Records of security issues being closed within SLA: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag are resolved within the SLA set in Vanta.

2 DOCUMENTS

Sample of remediated vulnerabilities

Vulnerability scan

Unique account authentication enforced

COMPLETE

The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.

7 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached.

Employees have unique email accounts: Verifies that every linked identity provider has more than one user.

Employees have unique infrastructure accounts: Verifies that every linked AWS and Heroku account have at least one user.

Employees have unique version control accounts: Verifies that every linked version control account has more than one user.

Service accounts used: Verifies that every AWS account is assigned a role.

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days.

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users.

Unique network system authentication enforced

COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

1 TEST

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

Article 33

Notification of a personal data breach to the supervisory authority

3 CONTROLS

Breach policy and procedure

COMPLETE

The company establish policies and procedures to respond to data breaches including notification procedures.

6 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta.

Company has an approved Incident Response Plan with GDPR Addendum and Breach Notification Procedures: Verifies that an Incident Response Plan with GDPR Addendum and Breach Notification Procedures has been created and approved within Vanta.

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan.

Employees agree to Incident Response Plan with GDPR Addendum and Breach Notification Procedures: Verifies that all relevant employees have agreed to the Incident Response Plan with GDPR Addendum and Breach Notification Procedures.

2 DOCUMENTS

Incident report or root cause analysis

Test of incident response plan

Incident management procedures followed

COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

5 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta.

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta.

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan.

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy.

Records of security issues being closed within SLA: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag are resolved within the SLA set in Vanta.

Incident response policies established

COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 DOCUMENTS

Incident report or root cause analysis

Test of incident response plan

Article 34

Communication of a personal data breach to the data subject

3 CONTROLS

Breach policy and procedure

✓ COMPLETE

The company establish policies and procedures to respond to data breaches including notification procedures.

6 TESTS

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Incident Response Plan with GDPR Addendum and Breach Notification Procedures: Verifies that an Incident Response Plan with GDPR Addendum and Breach Notification Procedures has been created and approved within Vanta. ✓

Employees agree to GDPR Compliance Policy: Verifies that all relevant employees have agreed to the GDPR Compliance Policy ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Employees agree to Incident Response Plan with GDPR Addendum and Breach Notification Procedures: Verifies that all relevant employees have agreed to the Incident Response Plan with GDPR Addendum and Breach Notification Procedures. ✓

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

5 TESTS

Company has an approved Incident Response Plan: Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

Company has an approved Operations Security Policy: Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Employees agree to Operations Security Policy: Verifies that all relevant employees have agreed to the Operations Security Policy. ✓

Records of security issues being closed within SLA: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag are resolved within the SLA set in Vanta. ✓

Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

Article 35

Data protection impact assessmen

2 CONTROLS

Determine needs and perform transfer impact assessment

✓ COMPLETE

If processing includes:

- systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- systematic monitoring of a publicly accessible area on a large scale.

1 DOCUMENT

Data Protection Impact Assessment (DPIA) ✓

Privacy impact assessment

✓ COMPLETE

The company performs a privacy impact assessment for processing or changes to processing, which represent a high risk to the rights and freedoms of data subjects.

1 DOCUMENT

Data Protection Impact Assessment (DPIA) ✓

Article 37

Designation of the data protection officer

1 CONTROL

Appoint Data Protection Officer

✓ COMPLETE

If processing meets one of these conditions then appoint a Data Protection Officer

- you are a public authority or body,
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data, or personal data relating to criminal convictions and offenses

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Article 38

Position of the data protection officer

1 CONTROL

Appoint Data Protection Officer

✓ COMPLETE

If processing meets one of these conditions then appoint a Data Protection Officer

- you are a public authority or body,
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data, or personal data relating to criminal convictions and offenses

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Article 39

Tasks of the data protection officer

1 CONTROL

Appoint Data Protection Officer

✓ COMPLETE

If processing meets one of these conditions then appoint a Data Protection Officer

- you are a public authority or body,
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data, or personal data relating to criminal convictions and offenses

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Chapter 5

Transfers of personal data to third countries or international organizations

Article 44

General principle for transfers

1 CONTROL

Identify basis for PII transfer between jurisdictions

✓ COMPLETE

The company identifies and documents its legal basis for transferring between jurisdictions.

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Article 45

Transfers on the basis of an adequacy decision

1 CONTROL

Identify basis for PII transfer between jurisdictions

✓ COMPLETE

The company identifies and documents its legal basis for transferring between jurisdictions.

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Article 46

Transfers subject to appropriate safeguard

2 CONTROLS

Basis for PII transfer between jurisdictions

✓ COMPLETE

The company's Master Services Agreement (MSA) informs the customer of the legal basis for transfers between jurisdictions and allows customers to object to changes or terminate service.

1 DOCUMENT

Data Processing Agreements (DPA) with customers ✓

Identify basis for PII transfer between jurisdictions

✓ COMPLETE

The company identifies and documents its legal basis for transferring between jurisdictions.

2 DOCUMENTS

Maintain data inventory map ✓

Publicly available privacy policy ✓

Article 48

Transfers or disclosures not authorised by Union law

1 CONTROL

Legally binding PII disclosures

✓ COMPLETE

The company rejects any non-binding PII disclosures. (SCC 15.2)

1 TEST

Company has an approved GDPR compliance policy: Verifies that GDPR compliance policy exists and approved in Vanta ✓

1 DOCUMENT

Data Processing Agreements (DPA) with customers ✓

Chapter 6

Independent supervisory authorities

Article 51

Supervisory authority

1 CONTROL

Appoint EU lead supervisory authority

✓ COMPLETE

If the company is operating in more than one EU state then identify a lead Data Protection Authority.

1 DOCUMENT

Lead supervisory authority appointed ✓

Appendix A: Definitions

Bug bounty program: A crowdsourcing initiative that rewards individuals for discovering and reporting software bugs, especially those that could cause security vulnerabilities or breaches.

DDoS: Distributed denial of service. A DDoS attack is attack in which multiple compromised computer systems flood a target—such as a server, website, or other network resource—with messages or requests to cause a denial of service for users of the targeted resource.

Multifactor authentication (MFA): A security system that requires multiple methods of authentication using different types of credentials to verify users' identities before they can access a service.

Penetration test: The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker might exploit.

Principle of least privilege: The principle of giving a user or account only the privileges that are required to perform a job or necessary function.

Protected data: Data that is protected from public view or use; includes personally identifiable information, sensitive data, HIPAA data, or financial data.

Sensitive data: Any information a reasonable person considers private or would choose not to share with the public.

SSH: Secure shell. A cryptographic network protocol for operating network services securely over an unsecured network.

SSL: Secure sockets layer. The standard security technology for establishing an encrypted link between a web server and a browser.

Appendix B: Document history

Vanta continuously monitors the company's security and IT infrastructure to ensure the company complies with industry-standard security standards. Vanta tests the company's security posture continuously, and this report is automatically updated to reflect the latest findings.

About Vanta

Vanta provides a set of security and compliance tools that scan, verify, and secure a company's IT systems and processes. Our cloud-based technology identifies security flaws and privacy gaps in a company's security posture, providing a comprehensive view across cloud infrastructure, endpoints, corporate procedures, enterprise risk, and employee accounts.

Vanta is based in San Francisco, California.