Groot 279: Security Policy

Overview

This IT security policy document explains how and why Groot279 collects, stores, uses, and shares personal data when you visit our websites or use our services. It describes the security policies in place at Groot279 to keep all data and assets within the Groot279 ecosystem secure.

“Personal data” in this statement means information specifically about users or used to identify users, including their identity, finances, and online behavior.

“Groot279” in this document means Groot279, Inc. This document mainly applies to the Groot279 application. To learn about our privacy practices for any of our other products or services, please visit the website and review the privacy statement for that particular product or service.

1. Privacy Policy

Our Commitment to Users’ Privacy

Groot279, a PayPal, Inc. service, respects and takes privacy seriously including users’ personal information and financial data. This privacy policy is applicable to all information we collect from current and past Groot279 users through our services. These services include, but are not limited to, any products, content, functions, websites, applications and services offered to you by PayPal, Inc. that are connected to a Groot279 account. As Groot279 is always improving, we may modify this privacy policy occasionally to update our changes. We will notify users of any material changes in the way their personal information is used by Groot279 by posting an announcement on our app or website, or by sending them an email. This privacy is made available on our website Groot279.com, and any questions or feedback can be sent to privacy@Groot279.com (Groot279).

Information Groot279 Collects

When a Groot279 account is opened, users are required to review our privacy policy and agree to our collection of your information in order to use our services. The information Groot279 collects from users is listed as below (Groot279):

- Account Information – device ID, telephone number, etc.
- Identification Information – user’s name, address, date of birth, email address, and governmental issued verification numbers such as SSN

- Device Information – IP address, device type and ID, geolocation information, time zone, browser type, language setting, and information of other machines with users' same payment cards that their machine ID is linked with for fraud prevention purposes
- Geolocation Information – their longitude and latitude coordinates through GPS or Wi-Fi for fraud and risk purposes or for service enhancement
- Social Web Information – data imported from social web services that users authorize to link with Groot279, including FourSquare, Twitter, and Facebook (credentials, email account information, friends list and public profile picture) for payment transactions and fraud prevention purposes
- Financial Information – online banking account information, routing numbers, and credit card information linked to Groot279 for transaction purposes. Groot279 does not share this information with third party social networking services.

For fraud prevention purposes, Groot279 may require additional information from users to verify their identify, address and other information such as their account transactions. geolocation information and access device to manage risks and compliance in order to provide a secure service for their transactions. However, Groot279 does not collect information of children under 13 years old as the services are not directed to them. Unless legally obligated to collect such data, we will promptly delete it. Please contact us at privacy@Groot279.com if you believe we have obtained information from a child below 13 by mistake. Users can also access and update their personal information at any time in your account settings (Groot279).

- **How We Use Cookies and Users' Personal Information**

When users visit Groot279's services or other third-party websites with our online services, Groot279 and our business partners may use Cookies for the following purposes (Groot279):

- Recognize them as a customer
- Customize our services, content and advertising
- Perform analytics
- Mitigate risk and prevent fraud
- Measure promotion effectiveness
- Promote trust and safety across the services

If users choose to disable or decline Cookies, certain services may be limited or unavailable. Do Not Track ("DNT") is an optional browser setting allowing users to choose preferences over tracking by advertisers and third parties. However, Groot279 does not respond to DNT signals (Groot279).

In order to provide users with a smooth, secure and customized experience, Groot279 may use their personal information for reasons as described below (Groot279):

- Offer services and customer support as requested
- Process transactions, collect fees and send notifications about transactions and network activities
- Troubleshoot and resolve problems
- Prevent potential fraud and illegal activities
- Create a connection between their Groot279 account and a third-party account
- Improve our services, content and layout
- Check for information accuracy and verify it with third parties
- Notify users of updates about our new products and services
- Perform compliance with law and regulations
- Enhance security of our services if users choose to share geolocation information with Groot279.

 How We Share Their Personal Information Within the Groot279 Network and With Other Parties (Groot279)

- In any circumstances, Groot279 does not disclose users' credit card number or bank account number to any party users have paid or that has paid them through Groot279 without their permission or requirements of a legal process. Groot279 also does not share users' personal data with third parties for marketing or promotional purposes.
- Users' public information such as username, profile picture, profile first and last name, account creation time, and related public transactions may be seen by anyone on the internet regardless of their having a Groot279 account. Their Groot279 friends list may also be seen by other logged-in users. This information may also be accessed and downloaded via Groot279's APIs or other third-party services associated with Groot279 products.
- Groot279 may share their personal data with:
  - PayPal, Inc., our parent company, and its subsidiaries for purposes allowed in this policy

- Companies that PayPal, Inc. plans to merge with or be acquired by with prior notice for customers
- Company or user they are paying or is paying them to process payments on Groot279 – users' contact information, date of sign-up, number of payments and other verification methods
- Vendors that Groot279 allows to accept payments from users – the vendor may share their information with us such as phone number and Groot279 username to let us confirm to that vendor that they are our customer and that we are allowed to serve as a form of payment for their purchase to that vendor.
- Law enforcement and government officials for legal purposes
- Service providers under contract for fraud prevention, payment processing, etc.

How Groot279 Protects Personal Data

- Groot279 uses third-party servers at data centers in the US to store and protect users' personal data with the following methods (Groot279):
  - Physical access controls to our office and files
  - Electronic and procedural safeguards
  - Administrative, managerial and technical safeguards
  - Computer safeguards such as firewalls and data encryption
  - Access allowed for only authorized employees to complete their duties
- In the event of a security breach, Groot279 may follow the below actions (Groot279):
  - Notify users electronically as agreed so that they can take appropriate actions
  - Post an announcement on our app or website
  - Email them using the email address they provided to us
  - Receive notice in writing (only applicable in certain locations)
- In addition, Groot279 also provides the following countermeasures to mitigate the risk of identity theft:
  - Allow privacy control options for customers
  - Replace SMS-based OTP with mobile-based authenticator app such as Duo mobile, RSA Keys, or Microsoft Authenticator
  - Evaluate alternatives to Facebook single sign-on
  - Enforce three-factor authentication
  - Explore an alternate architecture to eliminate open API
- We consider taking the below actions to prevent financial theft:
  - Encrypt all communications using HTTPS using AES 128-bit ciphers

- Adhere to all the best practices and regulations for corporations in the financial sector
- Provide fraud detection mechanism
- Require one-time authentication code in P2P transactions
- Explore controls and reporting processes to recover wrongly sent funds

- Groot279 plans to take appropriate steps to avoid reduced consumer confidence due to lack of privacy protection as follows:
  - Provide and allow customers to access policies of their data
  - Allow options for customers to publicize your transactions instead of automatically generating a post about their transactions
  - Provide transparency on the use of customers' personal data
- In order to protect users' data, Groot279 complies with the following data protection legislations:
  - Gramm Leach Bliley Act (GLBA)
  - California Consumer Privacy Act (CCPA)
  - US Federal Trade Commission (FTC)
  - Fair Credit Trading Reporting Act
  - Payment Card Industry Data Security Standard (PCI)
  - Sarbanes-Oxley (SOX)
  - Health Insurance Portability and Accountability Act (HIPAA)

User Responsibilities

- It is the users' responsibility to review our privacy policy periodically to stay updated of our changes. Groot279 will post announcements and send them notifications of our updated policy.
- Regardless of Groot279's countermeasures to protect our system security, we cannot guarantee their personal data may not be at risk due to security breaches. Groot279 recommends users take precautions to protect their personal data and never share their Groot279 password with anyone (Groot279).
- Users have the responsibility of securing their personal information using protective actions such as avoid sharing their credentials or device with someone else and notifying Groot279 as soon as possible once they think their account has been compromised.
- Users should refrain from all transactions for potential illegal purposes and all activities that affect the confidentiality and security of other Groot279 accounts.

- **Violations of Privacy Policy**

Users are required to agree to and accept the terms of our privacy policy before they can use our services. Violations of our policy may lead to fines or charges:

- Their account may be suspended or terminated in the event of a suspicious activity.
- Fines and charges as a result of illegal activities depending on the level of severity.
    - Identity theft: A violation of identity theft can range from 180 days to two to ten years in jail and/or a fine of up to $10,000 (Identity Theft).
    - Financial theft: Charges of financial theft depends on the level of severity and amount of transactions involved.

2. Physical Security Policy

This policy is crucial to protecting Groot279 information assets in the data center locations where they are housed and protected. Specifically, this policy ensures the protection of information assets from *theft* and *physical damage* at data center locations. Groot279's parent company PayPal, Inc., has contracted Digital Realty Trust for the provision of data center services to support Groot279 business functions. As data center provider, Digital Realty Trust will be required to follow strict adherence to PayPal, Inc. requirements on data center compliance.

- **Data Center Compliance**

- The data center provider must always have a valid Service Organizations Control 2 (SOC 2) report available. This is also known as the "Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy," based on the stated guidelines from the American Institute of Certified Public Accountants (AICPA). This is critical to meeting PayPal Inc.'s requirement for reliable Trust Services to address IT-enabled risks ("Data Center Compliance, n.d.).
- Enforce PCI-DSS Compliance Standards, as articulated in Section 1.
    - Section 2 Physical Security Policy emphasizes PCI-DSS Requirement 9: Restrict Physical Access to Cardholder Data. As stated by the PCI Security Standards Council (2018), the following controls will be emphasized:
    - *9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. 9.2 Develop procedures to easily*

distinguish between onsite personnel and visitors, such as assigning ID badges. 9.3 Control physical access for onsite personnel to the sensitive areas. Access must be authorized and based on individual job function; access must be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. returned or disabled. 9.4 Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained, given a physical badge or other identification that expires and identifies visitors as not onsite personnel, and are asked to surrender the physical badge before leaving the facility or at the date of expiration. Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name, company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law. 9.5 Physically secure all media; store media back-ups in a secure location, preferably off site. 9.6 Maintain strict control over the internal or external distribution of any kind of media. 9.7 Maintain strict control over the storage and accessibility of media. 9.8 Destroy media when it is no longer needed for business or legal reasons. 9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This includes periodic inspections of POS device surfaces to detect tampering, and training personnel to be aware of suspicious activity. 9.10 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties. (p. 20-21)

- The data center provider must always have a valid Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, available. This is based on AICPA guidelines (Triplett, 2015).
- The data center provider must always have a valid SOC 3 report available.

- **Data Center Security** ("Secure Data Centers," n.d.)

  - Comprehensive 24/7 CCTV monitoring with digital backups and remote access.
  - Smart-Card readers with biometric authentication mechanisms for on-site access.
  - Strict identification and authorization protocol for on-site visitors.
  - Secured data center cages, using ground bolted cage frames, reinforced steel wire mesh, Smart-Card biometric access, and climate-controlling HVAC system.
  - Fortified building construction.
  - Tested emergency preparedness planning and reliable back-up power in case of electrical outages.

- Physical intruder detection and prevention mechanisms, including on-site physical security personnel present 24/7, motion-triggered floodlights for night visibility, and two-tier perimeter fencing with checkpoints for entrance authorization.

- **Violations of Physical Security Policy**

- Data center providers who violate the agreed upon terms for Compliance and Security may incur a termination of contract, billing for any incurred damages as a result of terms violations, and potential civil litigation.
- Trespassing on the data center site is punishable by fines and penalty prosecution, depending on the state of the violation. Trespassers may expect $75 to $250 for a first-time offense, up to $2000 for repeated offenses, and a minimum of 16 months imprisonment for felony violations (Seidel, 2019).
- Theft of any assets from the data center will be reported to state authorities for prosecution, with fines ranging from $100 to $300,000 or more, depending on the nature of the crime (Penal Code, Title 7. Offenses Against Property Chapter 33. Computer Crimes).

3. Business Continuity Policy

Groot279 understands that customers rely on us to navigate their daily lives when it comes to making funds available for use and keeping track of their daily expenses and other financial obligations. To this end, Groot279 Inc, has defined the following robust Business Continuity Plan (BCP) and implemented it across the organization, not only to meet regulatory requirements but to exceed them as well.

The details of which are defined below:

- **Internal network outage**

- Groot279's IT team has designed the entire network to be free of any single points of failure. This means that there is redundancy built into the network circumventing network outages due to most device failures.
- All routing and switching protocols in use across the network have built-in failure recovery mechanisms which further strengthen the resilience of the Groot279 network architecture.
- Change management procedures are designed to prevent any major network changes from being done during business hours. This is intended to prevent any issues from network configuration changes taking down the network during periods of heavy traffic.

- And all Groot279's datacenters have back-up power generators which can power the entire datacenter in the event of a power outage.

Internet connectivity outage

- Internet connectivity at all Groot279 offices and datacenters is provided through two disparate service providers. This is to ensure that a ISP-level outage does not affect connectivity and an automated switchover mechanism is in place to redirect all traffic through the active provider in the event of an outage with one of the providers.
- Also, each of Groot279's two datacenters has a secondary disaster recovery site. Each of these locations has two separate internet connections for redundancy.

Denial of Service

- In order to ensure availability of the Groot279 application in the event of a Denial of Service attack against the Groot279 network, all servers have a redundant backup server in order to maintain connectivity.

System failures or interruptions due to natural disasters

- All systems are constantly upgraded to run the most stable versions of software as well as any relevant hardware upgrades. This ensures that the system architecture is reliable as well as optimized for performance.

Violation of the Business Continuity Plan

- In the event of any violation in the BCP policy, the personnel responsible are required to immediately follow the escalation procedure to flag the discrepancy to their immediate supervisor. In case there is no response or change of status to full compliance within 60 minutes, the issue shall be escalated to the VP of operations with every further delay of 30 minutes requiring further escalation up the hierarchy chain with the CEO being notified of this event within 120 minutes of the initial report.

4. Information Security Policy

Groot279 is extra careful about the issues related to information security as information leaks and malicious software can affect our customers and may result in degrading their trust in our service.

- Groot279 systems are equipped with highly efficient anti-virus software which are the part of policy for protection of customer's financial information and to protect them from any kind of malicious activity.

This software is updated time to time with renewal of license, any system with outdated virus detection software or expired license gets taken care of immediately with due action taken against the employee for negligence.

- Groot279 keeps track of every transaction and transfer of information transfer. Every transaction is followed by a confirmation message. If the receiver of these transaction is not authorized or is someone who is not intended to receive that transaction, the transaction gets revoked. However, if the sender confirms the transaction, Groot279 will not be held responsible for any amount lost.
- Groot279 keeps track of all the IP address keeping in mind the privacy policy of Groot279,
  all the IP address and registration details should match and if login details matches with the correct answers of security questions only then the access will be granted in case any of the detail is incorrect then access will not be given to the user.
- Groot279 network gets checked by our network engineers every week to check vulnerabilities and loopholes in our network, in case any such condition occurs entire network shutdown will take place and all the users will be informed on their registered mobile number, and all the transaction will be paused for a time being.
- On Groot279, we provide 24 hours customer service with one recall officer present all the time to protect customers from any kind of fraud, if any customer gets targeted to fraud and report within time, the amount will be reverted to the customer's account and a complain will be filled against the receiver of the amount, in case of guilty the customer's privileges will be revoked with immediate termination of account.
- All systems on Groot279 are equipped with personal firewall, Anti-virus and spam filters which help to reduce footprint and make the systems more secure for use. In any case of software vulnerability, that system immediately goes for software updating putting backup systems in use.

In case of any such activity encountered, Groot279 will close its services for a time being, to make sure all the transaction happening post the incident are safe to proceed with and will notify all the users so that customers can get aware of on-going difficulty and can be assured that they are in safe hands.

5. Employee Code of Conduct Policy

Groot279 believes an effective Employee Code of Conduct (ECoC) Policy is critical to building a defense-in-depth mindset within the organization's culture. The ECoC outlines critical behaviors for employees to make sure they do not become liabilities for the company and its customers. The ECoC outlined in this Security Policy document requires employee behavior which will protect the confidentiality, integrity and availability of Groot279 information assets.

- **Employee Communication Protocols**

  - All employees are required to only use their Groot279 provided email account for any company-related email communications.
  - Any emails received from a non-company email will be flagged as such in the email application, with a strict warning advising employees that this email has come from outside the company and must be opened with caution.
  - Install additional anti-phishing software to automatically filter out potentially malicious emails.
  - Employees must attend a biannual training on phishing campaigns, spear phishing campaigns, and social engineering attacks. This training will be provided by the Human Resources Department in conjunctions with the IT Department.
  - All employees are prohibited from disclosing system critical usernames and passwords over telephone, VoIP, or other telecommunications technologies.

- **Employee Internet Use**

  - Site blocking software will be used to block access to any flagged or malicious sites.
  - Site blocking software will also be used to block access to non-productive sites, e.g. YouTube, Facebook, Twitter, etc., unless access to such sites is required by the position of employment.
  - Employees are strictly prohibited from downloading content from non-work related sites. Access to any blocked websites that are necessary for downloading or uploading information will need to be approved by the Human Resources Department and the IT Department.
  - Employees are strictly prohibited from intentionally downloading or installing malicious software onto Groot279 information systems.

- **Employee Termination Protocols**

    - Employees who are to be terminated will be given a 2-week notice prior to final termination. Any system privileges will be reduced to visitor system privileges immediately. Visitor system privileges will have the lowest access, allowing soon-to-be terminated employees enough computer access to continue working during their last two weeks.
    - Once the 2-week termination period ends, all system access for the terminated employee will be immediately revoked. Authorization to physically access Groot279 offices will also be immediately revoked.
    - The Human Resources Department and the IT Department will conduct a review of employee activity logs for terminated employees for at least the 2 weeks prior to full termination.

- **Violations of Employee code of conduct**

    - The use of non-Groot279 email accounts for the communication of any company information is punishable with a formal HR review, temporary work suspension without pay, and possibly termination depending on severity of the violation.
    - The downloading or installing of malicious software onto Groot279 systems is punishable with immediate termination of employment. In addition, Groot279 will report the malware violation to state authorities for prosecution, with fines ranging from $100 to $300,000 or more, depending on the nature of the crime (Penal Code, Title 7. Offenses Against Property Chapter 33. Computer Crimes).
    - It is the Human Resources Department's responsibility to enforce the Employee Termination Protocols, and failure to enforce these protocols will result in a disciplinary review of the responsible department staff, conducted by upper level management.
    - Employees who continue to have unauthorized access to Groot279 information systems after termination will be held liable for damages pursuant to state penal codes on computer crimes (Penal Code, Title 7. Offenses Against Property Chapter 33. Computer Crimes).

6. Acceptable Use Policy

Users have the responsibility for complying with all the applicable laws and regulations associated with their transactions. They are also required to agree to the terms of our Acceptable Use Policy before using our services as follows:

- Groot279 plans to work with mobile platform providers such as Google and Apple to prevent the Groot279 app from installing unless it is on a minimum version number.
- Groot279 engineers the app to run in a sandboxed environment irrespective of the mobile platform it is installed on.
- All business usage on Groot279 has to be authorized.
- Groot279 provides seller and buyer protection.
- Groot279 collaborates with banks and agencies to set up anti-money laundering programs
- Groot279 sends our customers warnings of unusual amounts or suspicious activities, items, senders or buyers.
- Groot279 offers a hotline for users to report suspicious activities.

In addition, users are required to refrain from the following prohibited activities:

("Acceptable Use," 2020)

- Violate any laws and regulations
- Involve illegal transactions related to prohibited substances and products that are harmful to consumers, drugs, cigarettes, stolen goods, discriminatory promotion and weapons
- Relate to payments of unlawful purchases that present a risk of fraud.

Violations of the Acceptable Use Policy:

- Groot279 encourages users to report violations of our policy to us either by email or hotline immediately.
- Under extreme circumstances involving suspicious activities that involve fraudulent transactions, Groot279 will contact users either by phone or email provided to us. If no response is given within one hour, Groot279 reserves the right to attempt to suspend or terminate the suspicious Groot279 account.
- Users who refuse to provide appropriate response as requested by Groot279 under such circumstances are subject to a fine of $200.

7. Change Management Policy

Groot279's entire operation relies on the availability of the payment services with an industry leading six-sigma uptime. And this change management policy has been defined in order to mitigate issues resulting from network architecture changes and configuration changes that could potentially result in downtime. In addition to an organization-wide policy of defining network changes in explicit detail as

well as testing any big changes before implementing them on the production network, the critical piece of this policy is defined below.

- **Change to network configuration that would result in non-compliance of regulations**

  - Groot279 mandates that all personnel shall follow the rigorously defined change management process in order to ensure that any issues with changes are detected during the planning phase itself and are not implemented in the production network. By following this process, not only can Groot279 safeguard against changes that will result in non-compliance, but also changes that result in issues that could otherwise have been prevented by due diligence.

- **Violation of the Change management policy**

  - In case of a violation of the change management policy, all involved personnel will be required to present a detailed report to a panel chaired by the CISO. And the panel shall have the authority to decide if there was a willful failure to follow the change management policy. The penalties can include (but are not limited to) punitive financial damages, termination and criminal charges.

References

Acceptable Use Policy. (2020, March 19). Retrieved April 12, 2020, from https://www.paypal.com/us/webapps/mpp/ua/acceptableuse-full

Data Center Compliance More Critical Than Ever. (n.d.). Digital Realty. https://www.digitalrealty.com/data-center-solutions/security-compliance/compliance

Identity Theft. (n.d.). Retrieved April 12, 2020, from https://www.matthoraklaw.com/criminal-defense/white-collar-crime/identity-theft/

PCI Security Standards Council. (2018, July). *PCI DSS Quick Reference Guide*. PCI Security Standards. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Penal Code, Title 7. Offenses Against Property Chapter 33. Computer Crimes. (n.d.). Texas Constitution and Statutes. https://statutes.capitol.texas.gov/SOTWDocs/PE/htm/PE.33.htm

Secure Data Centers Support Operational Efficiency. (n.d.). Digital Realty. https://www.digitalrealty.com/data-center-solutions/security-compliance/security

Seidel, Michelle. (2019, December 9). *California Trespass Law: Criminal Trespassing, Charges, and Penalties.*. Legal Beagle. https://legalbeagle.com/13720956-california-trespass-law-criminal-trespassing-charges-and-penalties.html

Triplett, Martin. (2015). *Security and Compliance in the Colocated Data Center: What You Need to Know*. Digital Realty. https://www.digitalrealty.com/blog/security-and-compliance-in-the-colocated-data-center-what-you-need-to-know

Groot279. (n.d.). Retrieved April 11, 2020, from https://Groot279.com/legal/us-privacy-policy/