Data Security

joinpanda.com

Panda: Secure and anonymous by design.

This document explains the Panda platform data security implementation and has been prepared by our data security team.

This covers the Panda mobile app, backend systems, and third-party systems. Third party systems refer to the data analytics providers used to track user behaviour, system performance, and report system crashes.

Please direct any questions to the Panda team.

Primary highlights:

- Data is encrypted at rest, and wherever possible user specific data (such as emails) are encrypted while hot.
- All data and systems are hosted on Heroku, a SOC2 and PCI compliant environment.
- We collect as little personally identifiable information as possible.
- We comply with HIPAA, POPIA, GDPR and other required data security regulations.

Secure by design

Vulnerability Monitoring

Panda systems have automated hourly and weekly security scans to ensure no upstream vulnerabilities and no live platform issues are undetected. We have a comprehensive bug bounty system in place for researchers.

Environment

Panda is a SOC2 Type-II certified company, our platforms are complaint with SOC2, PCI-DSS, HIPAA and other relevant virtual and physical security requirements.

Compliance

Panda has a full-time head of Legal and Data Protection Officer ensuring our compliance with standards such as GDPR, POPIA and other data protection needs.

Infrastructure

Panda has a cloud-based backend (this includes databases) that is hosted on **Heroku.** All data that is used by the platform is **encrypted** in transit and at rest *(where it is stored)*. The app makes use of a **PostgreSQL** database and a **Redis** in memory datastore.

This infrastructure backend is SOC2 compliant, and access to the Panda team is restricted based on a seniority and needs basis.

Data Types

The platform consists of the following data:

1. **User Information** - This is data specific to a user of the app (a person using the platform to access mental health related services and resources)
2. **Mental Health Professional (MHP) Information** - This is data specific to a mental health professional user (a person using the platform to provide mental health services)
3. **Platform Specific Information** - This is information used by the platform for functionality.
4. **Mental health content** - This is content shared in the life skills section.
5. **Public Information** - All information available to the public.

User Information

One of the platform's main requirements is to provide as much anonymity to a user as possible. This results in the platform soliciting as little information about the user as possible on sign up. Data stored about a user:

1. An alias/nickname - name a user will identify as on the platform.
2. Gender (optionally selected)
3. Age group - An age range selection (e*xample 25-34)*
4. Mental health topics of interest
5. Profile picture (predefined platform image or user uploaded image)
6. Email address
7. User comments (made during a Forest session)
8. User ratings (ratings a user gives a MHP or a specific Forest session)
9. User notes (notes a user keeps for journal entries)
10. Scheduled appointments (with MHP)
11. Assessment scores
12. Payments
13. Medical aid details
14. Promocodes
15. Tags

All user information is kept confidential and only the user's platform generated id and components of the email address are used for platform analytics **only when the user has given consent**. More sensitive information about the user (i.e., medical aid details) are only obtained when the user wants to use more personal MHP services, like a 1:1 consultation with an MHP.

A user can sign up to the platform in the following ways:

1. **Personal email** - a user can sign up in a personal capacity using their email address and providing the required details.
2. **Promo code -** a user can also provide a promotional code, provided by certain organisations, which will then unlock access to certain services that fall behind paywalls.
3. **Tags** - Using deeplinks a user can be tagged as part of a particular organisation, that is in partnership with Panda, which will then grant them access to that organisation's benefits.
4. **Domain** - A user can use a work email address and if the domain belongs to a Panda partner organisation, the user unlocks the specific benefits that have been provided organisation. *Note: emails are verified before a user is granted access to the app. As a result, the email address must exist for a user to get the verification link to set up their profile.*

Once signed in, a user can only access their own data via a secure JSON web token (JWT). The only information they can view in relation to another user is an alias during Forest sessions, and comments by other users during a Forest session. The token has a time to live, and upon expiry a re-authentication is required by the backend. The user also has a view of certain MHP details that will assist them in making a choice of which MHP they would like to.

When a user deletes their Panda account, all their personal information is then anonymised. This means that their information is "hashed", and profiles are deactivated on our side once they delete their Panda account. We do not fully delete their profile to ensure that reporting and analytics are not impacted. By jumbling/hashing the user information, we can ensure that user's data remains inaccessible whilst still being able to aggregate data where required. This is compliant with GDPR and POPIA regulations.

We do not access or keep any medical records in our system or in the Panda app. Users do not give us any permissions to access this information and we are not integrated with any Medical Aid schemes or MHPs on this level. In our app, users can do assessments to help them better understand how they're feeling and what help they need.

Panda may share assessment results with MHPs or counsellors, however, users must give explicit permission to do so. The reason for the sharing of assessment data with MHPs or counsellors would solely be for them to analyse the results to offer the best possible care. Once this information is shared with the permission of the user, MHPs will be bound by their usual doctor-patient confidentiality agreement.

When sharing statistical information with partners, we only share the number of users completing assessments, or generalized and anonymised information. There is no way for a partner or company to delve into that information to see which users are completing which assessments. This allows us to uphold the anonymity for our users, while providing the client with useful information.

Mental Health Professional (MHP) Information

To register as a MHP on Panda, we require additional information, which in turn requires verification by Panda. This information includes:

1. Full Name
2. Email address
3. Phone number
4. Profession
5. Areas of expertise
6. Professional photo
7. Accreditation document
8. Practise address
9. Google or Microsoft calendar authentication details
10. Time slots available for bookings
11. Session details (Information on the type of sessions they will be offering on Panda)
12. Banking details

One the MHP provides us with the information numbered 1-3 and we successfully confirm their email address, the MHP can than browse the app/platform but will not be able to provide any MHP services until they are verified. In order for MHPs to provide services all information from steps 1-12 must be completed and their professional certification, affiliation and practice numbers must be verified by our Panda Administrators.

Auditing

The Panda API backend is scanned weekly by a 3rd-party security testing firm, and the source code scanned hourly for any vulnerable upstream packages.

Panda contracts with MWR in South Africa to complete our full penetration tests of the platform, Enterprise clients may request the most recent copy at any time.

Panda has a full time GDPR data protection officer and CISO, as well as a comprehensive bug bounty policy for working with security researchers.

This document was last updated on the 17th of August 2023.