Grokker GrokkyAi™ Safety & Security FAQ

1. **What personal information will GrokkyAi collect?**
   GrokkyAi is designed with your privacy and security in mind. We collect a limited amount of personal information to ensure the functionality and continuous improvement of our services. This includes:
   - **Account Information:** We collect the email address associated with your account for authentication and communication.
   - **Interaction Data:** Your chat conversations and usage logs are retained for a defined period. This allows for a more contextual and effective interaction with GrokkyAi and helps us to troubleshoot and enhance the service.
   - **Integrations for Enhanced Functionality:** GrokkyAi can integrate with other systems to provide more comprehensive assistance. This may include accessing data related to your employee benefits, eligibility for those benefits, or your Grokker account.

   All data is handled in accordance with strict security protocols to ensure its confidentiality and integrity.

2. **How will this information be used?**
   The information collected is used to enhance the member experience. GrokkyAi leverages anonymized conversations and app usage data to improve the overall quality of the responses.

   GrokkyAi also leverages member benefits eligibility data to provide personalized member benefits guidance. We are committed to responsible data stewardship and maintaining a clear separation between the data used for personalization and the anonymized data used for system-wide improvements.

3. **Will this information be shared with any third parties?**
   Your personally identifiable information is not for sale or for sharing. Our commitment is to you and your privacy. However, Grokker may share aggregated and anonymized data about GrokkyAi usage with our partners for purposes such as analytics, technical support, and research, but never in a way that could identify or compromise any individual user.

4. **How long will this information be retained?**
   We are committed to protecting your privacy by minimizing how long we store your personal data. Your personally identifiable information is permanently anonymized within one year after your contract with us ends.

   We keep your account data for this short, one-year period for necessary final support or administrative purposes. Once that period is over, we follow a strict process, guided by HIPAA privacy standards, to permanently remove all of your personal identifiers (like your name, email, and any protected health information).

   The remaining anonymous data may be used to help us improve our services, but it has no connection to you and can never be used to identify you.

5. **What measures are in place to ensure the accuracy and integrity of the data collected?**
   Grokker ensures data accuracy and integrity through anonymization, secure storage, strict data handling procedures, and regular monitoring and audits, safeguarding both member privacy and the quality of the data collected.

6. **How will GrokkyAi handle sensitive health information or mental health concerns?**
   In case of emergency, GrokkyAi strongly encourages people to seek help from qualified healthcare professionals for any sensitive health or mental health concerns. If you share such information, it will never be exposed to other users or used to train any AI model.

7. **What measures are in place to ensure GrokkyAi provides accurate and safe information and recommendations?**
   GrokkyAi prioritizes providing accurate and safe information by curating its responses from Grokker's trusted expert-created content library, actively monitoring and rating its performance, encouraging user feedback, and continuously improving its capabilities.

8. **Can GrokkyAi connect users to a live person if needed?**
   GrokkyAi does not currently offer live handoffs to human support within the chat. However, if users need further assistance, they can contact Grokker's support team directly at support@grokker.com for help.

9. **How is my information kept separate from other users?**
   Your privacy is paramount. We prevent any crossover of user information through a robust security framework. Each chat occurs in a private, end-to-end encrypted session that isolates your conversation. Your data is strictly segregated and is never used to inform another user's session or for AI training. We combine this with industry-standard encryption for all data in transit and at rest, along with strict internal access controls, to ensure your information remains confidential and visible only to you.

10. **How do you store and protect my data from unauthorized access?**
    We are deeply committed to protecting your data through a multi-layered security framework that safeguards it from unauthorized access, use, or disclosure. Our approach is built on the following pillars:
    - **Secure, World-Class Infrastructure:** All our systems are hosted on secure servers provided by Amazon Web Services (AWS), a leading cloud provider that meets the highest international physical and technical security standards.
    - **Comprehensive Encryption:** Your data is encrypted at all times. It is encrypted in transit (as it travels over the internet) and at rest (while stored). This renders your information scrambled and unreadable to any unauthorized party.
    - **Strict Access Controls:** We operate on a "principle of least privilege." Access to user data is strictly limited to a small number of authorized personnel who need it for specific, necessary purposes like system maintenance.
    - **Proactive Monitoring & Audits:** We don't just protect against current threats; we prepare for future ones. We use continuous monitoring and conduct regular security audits to proactively identify and address potential vulnerabilities.
    - **A Culture of Security:** Our team is your first line of defense. We provide ongoing training on data security best practices and our information security policies to ensure security is embedded in everything we do.
    - **Secure Data Deletion:** When data is no longer needed, we follow a strict protocol to ensure it is permanently and securely destroyed.
    - **Incident Response Readiness:** In the unlikely event of a security incident, we maintain a comprehensive incident response plan to ensure a swift, effective, and transparent response to protect your data.

    These measures work together to create a robust security posture that ensures the confidentiality and integrity of your information.