13 Point Checklist

For appraising AI apps

Ensuring that an AI app handles your information correctly and does not share it inappropriately involves several steps and considerations:

1. Review privacy policies and terms of service:

Start by reading the privacy policy and terms of service of the AI app or platform. Look for information about how they collect, use, and share your data. Reputable companies should have clear and transparent policies in place.

2. Data encryption:

Ensure that the AI app uses encryption to protect your data during transmission and storage. Look for mentions of SSL/TLS encryption for data in transit and encryption-at-rest for data stored on their servers.

13 point checklist for appraising AI apps

3. Access controls:
Check if the AI app implements robust access controls and authentication mechanisms to restrict access to your data. This includes role-based access control (RBAC) and strong password policies.

4. Compliance with regulations:
Verify if the AI app complies with relevant data protection regulations such as GDPR (for European users), HIPAA (for healthcare data), or other regional and industry-specific standards. Compliance indicates a commitment to data privacy.

5. Data handling practices:
Investigate how the app handles your data once it's processed. Does it retain your data indefinitely, or is it deleted after a certain period? Make sure the app's data retention policies align with your expectations.

6. Third-party integrations:
Be aware of any third-party services or integrations the AI app uses. These may have their own privacy policies and data-sharing practices that could impact your data.

7. User permissions and consent:
The app should request your consent before collecting and processing your data, especially for sensitive information. Ensure you understand what you are agreeing to when you use the app.

8. Data access and deletion:
Check if the app allows you to access your data, correct inaccuracies, or delete your information from their systems upon request. These features are often required under data protection regulations.

13 point checklist for appraising AI apps

9. Security audits and certifications:
Look for evidence of security audits, certifications (e.g., ISO 27001, SOC 2), or independent assessments that attest to the app's security and privacy practices.

10. User reviews and reputation:
Read user reviews and comments about the app's privacy practices and any past incidents of data breaches or privacy concerns. A good reputation for privacy is a positive sign.

11. Contact information and support:
Ensure that the app provides a way for you to contact their support or privacy team if you have questions or concerns about your data.

12. Regular updates:
Revisit the privacy policy and terms of service periodically. Privacy practices can change, so it's essential to stay informed about any updates.

13. Limit data sharing:
Whenever possible, minimise the amount of personal information you provide to the AI app. Only share the data that is necessary for the app to function effectively. There’s further information and guidance in this article – the dos and don’ts of sharing sensitive information.

If you have concerns about an AI app's data handling practices or suspect a breach of your privacy, you can contact the app's support team, the platform hosting the app (e.g., Apple App Store, Google Play Store), or relevant data protection authorities to report your concerns and seek assistance.

Contact us:
support@itg.uk.com
01625 613 633
www.itg.uk.com

IT Support
Cloud Services
Cyber Security
Telecoms
Web Development
Search Marketing