We need to identify who you are and use Google's sophisticated authentication system for that purpose only. If you already have a Google identity (for instance a gmail account) you can use that.

Additionally, we use Google’s infrastructure (servers and security) to store your data in the Cloud. Your data will be stored in encrypted form only. This means that your data is not stored as readable or clear text on any server.

Your data will be encrypted before leaving your device. The data is transported over the Internet in encrypted form using a secure connection. It is then stored in encrypted form on secure servers.

We use a highly secure form of encryption before any data leaves your device. The data is encrypted using your Krypta password. This should be a strong password you can remember well (it’s the master password for all your data). There is no way to recover your data in case you lose your Krypta master password. You can make an unencrypted backup of your data to put somewhere in a safe place.