With Otto security and privacy

Security and privacy are key considerations for everything we do and we've taken steps to ensure that your data, and that of your clients, is safe. This guide explains some of those steps and can also be shared with your clients so they know their data is in good hands.

Otto

Unique to your practice
Each practice has its own Otto, who only works within that practice. Data is not shared between practices.

You have full control over access to clients
As with any other member of your team, Otto's access to clients is managed through your Xero HQ account. Otto can only access a client if he has been given access. You can add and remove access to your clients at any time.

Access to Xero
Otto accesses Xero via a browser and logs in just like you do. His password is randomly generated and consists of a mix of upper and lowercase letters, numbers, and symbols. 2FA is enabled. His login details are securely stored and encrypted.

We recommend providing Otto with a Xero role that offers the minimum access possible. This is **Standard** for regular Xero business plans, and **Advisor** for partner-only plans such as Ledger and Cashbook.

Otto runs on Amazon Web Services (AWS) servers in their London data centre. Training is performed on on-premise hardware in Cambridgeshire, UK.

Training and reconciliation data
The information used to train Otto, as well as the information displayed in the portal, is stored in a database hosted by Supabase. This data is stored in an AWS data centre in London.

All information used by Otto and the portal is stored in a single database and access permissions ensure practice staff can only see information for their practice.

12 months of reconciliation data are downloaded when you assign a client to Otto so he can be trained. Every fortnight, new reconciliation data since the last training will be downloaded. The volume of training data increases each month because Otto's decisions are generally more accurate if he has more examples to work with.

The data used to train Otto is comprised of the following:

Bank statement	**Bill, invoice, or transfer**
• Unique ID generated by Xero	• Unique ID generated by Xero
• Transaction date	• Issue date
• Payee	• Contact name
• Reference	• Reference
• Description	

The portal

The portal is where you can view the work Otto has done, provide feedback, and manage all the settings that control what Otto will do for each of your clients.

It is important that you create a strong password that you don't use elsewhere. We also recommend using a password manager. The portal supports multi-factor authentication using authentication apps, such as Google Authenticator, and Passkeys, a recent standard that uses technologies such as fingerprints and face recognition on your phone and laptop for extra security.

The portal accesses the database using a unique username and password, over an encrypted connection. The server is hosted by Hetzner in their Falkenstein, Germany data centre. A network firewall ensures that only web traffic will be received by the server. Any administrative and maintenance activities can only be performed by a specific user when connecting from a specific IP address.