With Otto security and privacy

Updated 18 July 2025

Security and privacy are fundamental to everything we do at With Otto. We've implemented comprehensive measures to ensure your data, and that of your clients, remains safe and secure. This guide explains our approach in clear terms and can be shared with your clients to provide transparency about how their data is protected.

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 you have 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. Two-factor authentication (2FA) is enabled, adding an extra security layer beyond just a password. 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–one of the world's most secure cloud platforms–in their London data centre. Training is also performed in AWS.

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, a leading secure database provider. 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. You can assign an appropriate role to each member of staff which can further limit the data that they are able to access.

When you first assign a client to Otto, we download 12 months of reconciliation data for training. Every fortnight, we add new reconciliation data, building up to a maximum of 18 months. After this point, we maintain a rolling 18-month window. Each day, any data older than 18 months is automatically deleted. This approach gives Otto the examples needed to make accurate decisions while ensuring we don't retain data longer than necessary.

To provide accurate reconciliations, Otto learns from specific, limited data points. Here's exactly what information we use for training:

Bank statement

- Unique ID generated by Xero
- Transaction date
- Payee
- Reference
- Description

Bill, invoice, or transfer

- Unique ID generated by Xero
- Issue date
- Contact name
- Reference

We also store transaction amounts in the portal to help you review Otto's reconciliation decisions. These amounts don't form part of his training.

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) for code-based security
- Passkeys – a modern standard that uses your device's biometric features (fingerprint or face recognition) for convenient, ultra-secure access

The portal accesses the database using a unique username and password, over an encrypted connection. The portal server is hosted by AWS in their London data centre.

Data location and privacy

Your reconciliation data is stored and processed in the UK. We use AWS London data centres for Otto's operations and Supabase's London facilities for database storage.

We also use third-party services to monitor system performance and identify technical issues. These services may store data in the EU. While we configure these tools to collect minimal data, such as redacting email addresses,, error reports could occasionally capture information visible on screen when an issue occurs (such as client names or other portal details.) We're transparent about this because, whilst rare, it's important you understand how all aspects of our system work.

Our commitment to transparency

We believe in being open about our security practices. Our full technical specifications and data protection details are available in our Terms and Conditions, and we're always happy to answer specific security questions from you or your clients.

If you have any questions about security or privacy, please don't hesitate to contact us at support@withotto.app