Letter of Authorization FAQ

What is the Letter of Authorization (LOA) and why does Concur need to obtain an LOA from a Customer?

Concur makes available a number of developer API, which allow third parties to connect their offerings to the Concur service. Many of Concur's Customers desire to work with these third parties to implement a tool or service that uses those API to connect with Concur service and enhance a Customer's use of a Concur service. This connection often includes the ability to access Customer data from the Concur Service by the third party through Concur's API(s). However, the services agreement between a Customer and Concur (Customer Agreement) prohibits Concur from sharing Customer's data with third parties. So, Concur needs explicit consent from Customer in order to share the data –without that consent Concur would be in breach of the Agreement. The LOA provides this explicit permission to make the data available and deals with certain other issues that follow from it. In short, the Customer's request for us to integrate with the third party necessitates us to share the Customer's data with the third party through our API, so (by the terms of our agreement with the Customer) we need the Customer's authorization to do so.

Can the Customer have Concur limit the data that is provided to the Service Provider?

Concur agrees that the data will only be sent by Concur's API, details of which can be found online at https://developer.concur.com/api-reference/index.html, so the release is not a blanket, unlimited authorization. However, the service provider, not Concur, is the party responsible for the development and use the connection. In other words, the service provider can call for the data, Concur does not send it to the third party. Concur cannot monitor the data exchange on a field level, so any specific controls and limitations must be between the Customer and the service provide, not Concur.

Why is the data transfer not part of the Concur service, as described in clause (b)?

The Concur service includes the element under control of Concur (or its authorized resellers), but that does not include the connector. The connector is developed and maintained by the third party service providers, and Concur cannot be seen as responsible for such connectors.

Why does Concur need the waiver in clause (c)?

The ability of Customer's third party solution provider to access data through the API to the third party solution is being made only because Customer has requested it and is not part of the services provided by Concur to Customer under the Customer Agreement. The Customer Agreement states that Concur will not share data outside of the Concur Service without permission of the Customer. This waiver provides the permission – without it Concur could be in violation of the Customer Agreement, and so would not 'flip the switch' to enable the connection.

Why does Concur need the indemnification in clause (d)? Doesn't the Customer Agreement already contain indemnification from Customer?

Once the data is made available to Customer's third party solution provider, it is no longer under Concur's control. Any issues concerning the data, how it is used, and any issues with the third party solution provider need to be addressed between Customer and the third party solution provider. The indemnity provided under the Customer Agreement does not cover issues arising out of the availability of data to Customer's third party solution provider.

If a third party files a claim against Concur relating to Concur's making the data available to this authorized third party solution provider at Customer's request, Concur should be entitled to seek protection from Customer. Such issue needs to be settled between the Customer and the solution provider – Concur no longer has control of the data and should not be held responsible for its use. Concur is relying on Customer's consent to release this data. If Customer does not have the authority to give such consent, Concur needs to be protected. Basically, in authorizing Concur to release Customer data to the third party, customer does so at its own risk and the Customer must hold Concur harmless against any damages that Concur may incur as a result of this data release (e.g., a claim by one of the data subjects). But – see the next question…

Does the LOA change anything under the Customer's Customer Agreement with Concur?

No. All protections under the Customer Agreement remain in place, including Concur's data responsibilities, and duty of confidentiality, except for the specific data released to the service provider under this consent. Concur is not asking for any change in the relationship as to data that remains in the Concur system, or for any information that is sent into the Concur Service by the provider.

Customer is working with a partner to implement a Single Sign On (SSO) solution. Does Customer still need to obtain an LOA?

It depends. For many Customers a simplified version of the LOA is available where Customer's data is not being made available (this has been provided to Concur's SSO platform members to be provided to appropriate Customers). However, if a Customer is working with an SSO provider to enable additional services that do require data exchange, like User Provisioning, then the full LOA is required.

Why doesn't Concur negotiate changes to the LOA?

These LOAs are standard and intended to cover almost all third party solution providers used by our broad base of Customers. This type of LOA is also very standard in the industry where APIs access is more and more a means of integrating services from unrelated companies. Concur needs to ensure that it has the permissions it needs and the risk allocation provisions it requires in a consistent manner.