Overview of **User Data Flow** through Go1 and 3rd Party Systems.

Version control

Author	Date	Version
Thomas Wythe	24/11/2021	v1.0
Thomas Wythe	25/11/2021	v1.1
Kanwaljit Dilawari	23/03/2022	v1.2
Kyle Jackson	30/10/2023	V1.3
Kristian Taylor	05/11/2024	V1.4

Introduction

This document describes the flow of user data through Go1 systems. This overview includes how data is transmitted to any 3rd party systems which also interacts with the same user data.

Go1 Content Marketplace

To set proper context: Go1 is a learning content marketplace of two sides.

On the supply side – Go1 consumes content from various e-learning providers (such as Skillsoft, Bizlibrary, Harvard etc.).

On the demand side – Go1 makes this content available to our customers, in a single solution.

Customers include: businesses of any size and 'distribution partners' who consume the Go1 content marketplace to enrich their own product offering for customers (i.e., learning management systems such as SAP SuccessFactors, Docebo, Oracle HCM learning who want to offer a rich content solution alongside the product features of their LMS).

In making learning content available to Go1 customers and their learners, it is necessary to collect, process and forward (to approved 3rd parties) some degree of personal data, to ensure the user learning experience is fit for purpose.

Principles of Data Transmission

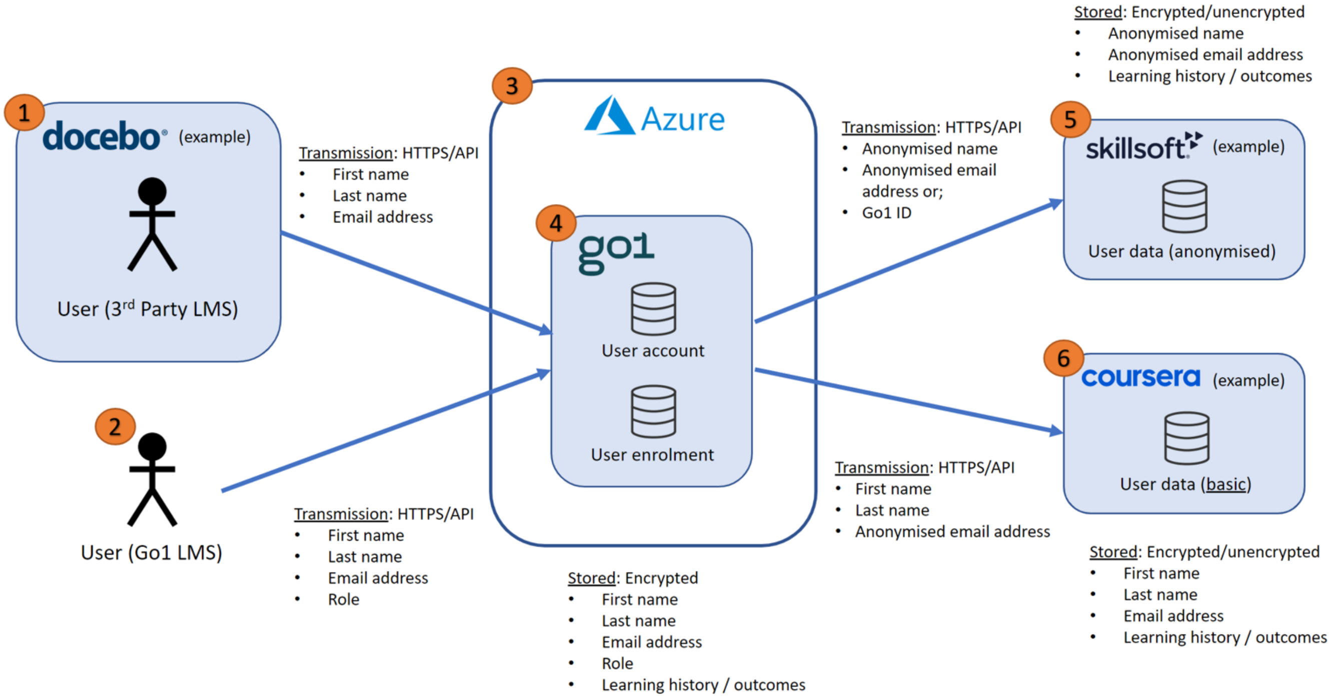
Go1 has defined a set of data transmission principles which govern what information is shared about a user, why it is shared and when.

These principles include:

- Only collect the data which is necessary to identify the individual and provide a relevant and contextual learning experience
- Only transmit the data which is necessary to ensure the user receives the best possible learning experience
- Any personal data transmitted to or from any Go1 system, should be encrypted in transit
- Any personal data which is stored within any Go1 system, should be encrypted at rest
- As new content providers are added to the Go1 marketplace, we must perform such due diligence as to ensure the proper treatment of personal data (should any data be stored by that 3rd party)

Overview

The illustration below is a visual representation of the Go1 data flow:



To assist with interpretation, each numbered item in the illustration is explained below.

Item 1: User in 3rd party LMS
In this case, Go1 content is accessed by an end-user from within a 3rd party LMS product.

Go1 content will be imported into this 3rd party LMS using either a native learning format (such as SCORM) or a simple metadata (title, description, image, duration – sufficient to inform learners of the contents purpose).

During the content import process, no user information is transmitted. Only when the content is opened, by the user, is any user information transmitted to Go1.

When the content is opened, the following is transmitted to Go1 via a HTTPS API call or through a SAML single sign on solution.

The data transmitted is minimized where possible:

- First name and last name
- Email address

Item 2: User directly accessing Go1
As noted, customers access Go1 either via a 3rd party LMS or directly, using the Go1 LMS web application.

As Go1 controls the experience within its own web application, some additional information may be able to be captured. This includes:

- First name and last name
- Email address
- Role or business function
- Topics of interest (i.e., business skills, leadership, taxation – used to determine their learning journey)

The transmission of this data is per item 1.

Item 3: Azure hosting infrastructure
Go1 uses Microsoft Azure hosting infrastructure with our primary region hosted in Sydney Australia. Customers do have the option of having their PII stored in either the US or EU.

Item 4: Go1 core platform
The Go1 core platform will receive user information from the 3rd party LMS or the Go1 LMS web application. This information is processed to provide a learning experience.

For example: 'as you are in the management team, your admin user has decided you need to take this training'.

All received data is stored and is encrypted at rest.

As the user takes a course, their outcome (pass, fail, complete and score against the course they took) is also stored, against their account profile. Therefore, their learning is linked to their personal information.

Item 5: 3rd party content provider – anonymized data
Several Go1 content providers have a real-time communication with Go1. These providers will host their own learning content and Go1 will use secure interfaces to seamlessly make their content available to users of Go1.

Most learning content providers do not require 'real' user information to function and provide a good learning experience. In these cases, Go1 will transmit an anonymized first name, last name and email address. For example:

- First name = ‘FIRSTNAME’
- Last name = ’LASTNAME’
- Email address = ‘GO_ACCOUNT_ID@MYGO1.com’ (this is not a real email address and there is no publicly available means to map the Go1 account ID to a real user) or;
- Go1 ID (the users unique, Go1 account ID which is not publicly available)

Item 6: 3rd party content provider
As per item 5, except this type of content provider will provide the user with some form of artefact, to prove their have completed the course or can demonstrate a competency. An example might include a digital or physical certificate.

Since the provision of this artefact is of value to the learner, Go1 will make the requisite information available to the 3rd party content provider to ensure the artefact is correct (i.e., the correct first name and last name appears on the certificate).

In these cases, the email address is still anonymized, and no other data is transmitted which is not essential to the process of generating the artefact.

Data security

Transmission of data

Data transmission between client endpoints and Go1 infrastructure is secured using TLS 1.2/1.3.

Data at rest

All data stored within the Go1 system is encrypted at rest, using Microsoft Azure Data Encryption which uses AES256 as the encryption key. Additionally, if username and password authentication is used passwords are encrypted using Bcrypt.