GDPR, Best practice from existing clients

Result of thorough investigation by big client (300.000+ employees):

It is alright to order and use the Actee Company subscription at Actee considering that:

- Actee offers an Actee Terms of Subscription considering the EU law.
- Your company does not handle any user nor user data.
- Your company can add your own training content and control it.
- Trainers (internal & external) and participants/trainees will register and fill in in their data either anonymously or specified with valid (Company or Non-company) email address on their own and their data will be deleted when they will delete their registration/user or anonymized when subscription are no longer active.

Actee.

Actee GDPR and data security – October 2022

Actee's handling of data in a few sentences in relation to the GDPR legislation:

Those of our clients' employees who play Actee or use any of Actee APS' digital tools can be logged into the Actee subscription as a guest by only entering a name (can be any fictive name).
(or the company's white-label version of this – which also comes in a free version).

To login the employee can register using a valid email-address as well as choose their own personal password (optional).

Passwords are encrypted and will therefore never be visible to Actee APS.

The email address is therefore the only account identifier at Actee APS. Signing up with an e-mail address is NOT mandatory but if an email is added the email address is stored in the systems' encrypted databases, and we do not share these emails or any other personal details with any undisclosed third party.

Which email is used is of no importance to Actee APS if it is personal and active.

Actee.

Actee GDPR and data security – October 2022

Optional and Derived data:

Only personal data to consider is the email the player (employee/end-user) can choose to fill in.
The player can also be allowed to use a fictive name and play as a guest.
If the player choses to add the email is enables to keep player profiles as part of the learning experience for the registered employees.

These plyer data are not sensitive and have the ”ordinary personal information” status in accordance with article 6 of GDPR legislation. The Actee system does not carry any sensitive personal information.

Derived data: When using the Actee subscription its games and tools, data is generated, and we call this derived data. We use this data to generate profile and data-views that are valuable to the user. This data is also anonymized and pooled to be used for comparisons with other users. Company clients (facilitators / program managers for example) can see the derived data of their attached employees inside Actee, in a aggregated manner.
If the user log in as guest this data will not be connected to any user and cannot be obtained at a later stage since the data is only connected to a fictive guest name.

Third parties, outside Actee APS, will never be given access to personal and/or derived data - in accordance with article 44 of GDPR legislation and the Actee Terms of Use.

Your existing LMS can potentially be allowed to integrate into the Actee system, but data will never be shared unless the individual end-user knowingly accepts this.

Actee.

Question / Potential issue	Answer
Autorization and access control to back-end systems	Only employees at Actee APS and their development team can get access to systems that contain data on clients' employees. All have signed NDA agreements and SCC's are in place.
Data with personal information	Data material in Actee APS' systems are deleted / anonymized so that it can never be linked up to the clients' employees again, if they choose to deactivate this data. For example, if they delete their account.
Logging of use	Actee APS' database setup at Microsoft Azure logs changes in the database.
User rights A) Right to deletion (article 17)	The signed-up user can always ask to get their account deleted with us. This will delete the account completely. At the same time, derived data will be anonymized for continued use by Actee APS. (Accepted with Terms of Use at sign-up.) All requests for deletion shall go to info@actee.com or you as a user can delete your own account under "Profile Settings".
B) Right to review account data (article 15)	The signed-up user can always ask to get a digital record of all the data associated with that said user. Derived data is included here. All requests regarding users' right to review shall go to info@actee.com.
C) Acceptance of our terms and withdrawal of these	Consent to our "Terms of Use" is given the first time you enter the system upon registration. Users can see their date of consent and review the terms under "Profile Settings" once logged in. Withdrawal of consent to the Terms of Use happens automatically upon request for deletion of the Actee account. In other words, you can't have access to Actee without consent is given.
D) Use of personal information for automatic profiling. (article 22)	Actee does not hold any sensitive information, since no such information is filled in by the user. Therefore no profiling based on sensitive information is done either. Actee does on the other hand use derived data in our system to send the user fitting messages and feedback on the user's actions. We only do this upon the acceptance of our terms of use.

Data Processor

Hosting:

Microsoft Ireland Operations Ltd. including group companies

Supplier of software services,
Hereby, but not limited to;
Microsoft Azure server setup

Actee APS' Azure cloud servers are placed in the Netherlands.

Actee is run on a "Public Cloud" setup. Off-premises, shared resources.

Address:

South County Business Park

One Microsoft Place, Carmanhall and Leopardstown

Dublin, D18 P521

Irland

Find more about Microsoft and GDPR here: ***https://www.microsoft.com/en-us/trustcenter/privacy/GDPR/solutions***

Company Specific Hubs

Seperate section to the Actee setup