DPIA Egodact software

October 26, 2019, Roermond, the Netherlands

This DPIA (Data Protection Impact Assessment) applies to the Agora ProgressMonitor and Agora ChallengeMonitor ("Egodact software").

Processed data
The amount of personal data that Egodact software processes is small; our software only processes the following data:

Type	**Processing optional**
Full name	No
E-mail address (as provided by the Google or Microsoft account)	No
URL of the profile picture of the Google or Microsoft account	No
Groups that the user has been assigned to or manages	Yes. Groups can be created and assigned to users by admins; Egodact is not involved in the management of these groups.

Note: "users" does mean all users; there's no difference between students and teachers in our software.

We also store the portfolios and portfolio histories of our users.

How we process this data
This data is processed in two ways:

- Through the user authentication system
- By storing it in our database(s)

We display this data in multiple places in our software; please read the privacy statement for an exhaustive list.

Why this data is processed and whether this processing is necessary

Type	**Why is processing this type of data necessary?**
Full name	If we don't store the full name of our users, we cannot identify them within our software.

	For example: teachers (coaches) select students in the coach mode to be able to view their portfolio. In order to do this, they need to know which student they are selecting.
E-mail address (as provided by the Google or Microsoft account)	We use e-mail addresses to authenticate users and to associate portfolios, history and other personal data with.
URL of the profile picture of the Google or Microsoft account	The processing of the URL of the profile picture is partially imposed by the user authentication system. It also helps in the recognition of users and is therefore useful as well.
Groups that the user has been assigned to or manages	It isn't; this type of data is only processed when you choose to assign groups.

The need for processing the portfolio and portfolio history is obvious; this is the actual functionality of our software.

Lastly, Egodact is fully GDPR compliant, since we are a European company. GDPR compliance is arranged through our data processing agreement.

Storing of data
Data is processed and stored in two ways (as mentioned before):

- Through the user authentication system (Firebase Authentication)
- All data is stored in our database(s) (Firebase Real-Time Database)

Both the database and the user authentication system use services by Google (Google Ireland Ltd.); these services are the Firebase Real-Time Database and the Firebase Authentication module. Firebase is part of Google.

This usage of Google services means that data is stored in the United States of America, which falls outside of the European Economic Area. Still, this storing of data is GDPR compliant since Google participates in the EU-US privacy shield and ensures GDPR compliance.

Retention period and modification of data
Egodact is not the "data controller" and therefore does not control when data is removed or modified. The school retains its responsibility to manage and control its data.

Do note that our usage of Google services causes a delay of (at most) 180 days in the deletion of data. During this period, Egodact cannot access the data, but it could still be stored on Google (Firebase) servers. This delay is imposed on us by Google/Firebase and we cannot change it.

Risks of data processing
The following two risks occur when using Egodact software:

- A data breach occurs (either on our behalf or Google's). This could lead to unlawful reading, modification or deletion of data.
- Google is forced by a (foreign) government to share data.

Impact of these risks
Should one of the above scenarios take place, the impact wouldn't be that great.

Since the amount of personal data that is stored by Egodact is small, the amount of breachable data is also small. This means that the risks for our users wouldn't be large, and that the consequences for the freedoms and rights of these users are also small if not negligible.

It follows that unlawful deletion or modification of data isn't a great risk either; although it could be tremendously inconvenient, in particular when portfolios or portfolio progress is deleted.
Do note that the personal data that we store of a user is reset to the personal data in their Google or Microsoft account when they sign in again.

Lastly, the chance that Google is requested by a (foreign) government to share with them the data that we've stored appears relatively small as well. And even if Google does get such a request, then that doesn't mean they'll oblige. Google claims to share as little data as possible (if any at all) with governments that request such sharing.

Certification
Google/Firebase is heavily certified. For example, it has an ISO27001 certificate.
You can view this web page to see what certification processes Google/Firebase services have completed: https://firebase.google.com/support/privacy/
Also, as mentioned, Google is GDPR compliant and participates in the EU-US privacy shield.

All of this reduces existing risks.

How are risks limited or reduced?
Egodact does not control to what degree Google has to share data with (foreign) governments. As a result, we cannot reduce this risk.

The risk of data breaches, on the other hand, can be reduced—data breaches on our behalf, that is. We achieve such reduction in the following ways:

- We carefully write and update the access rules of our databases. We always keep privacy and security in mind when adding new features, meaning these rules stay up-to-date.
- Each school has its own database. We also treat the passwords of the Google accounts we use to access Google services with great care; only people who have to access these passwords will get such access. With these people, we've either signed

non-disclosure agreements, or they're obliged through other agreements with Egodact or by the law to keep information secret.
- We use a system of user authentication to ensure personal data is only lawfully accessed (read the next section for more details).

User authentication and user roles
First of all: users always have to sign in before they can access any of the personal data we store. This personal data is never accessible for the outside world.

Our software also knows the following user roles:
- Student (Basic user; can only access and modify their own portfolio and its history.)
- Coach (Like a student, but can also access portfolios and portfolio histories of any other user. Note that coaches can only view, comment on and move the coach rubric sliders in portfolios. They cannot actually modify anything that the portfolio owner has inserted.)
- Editor (Like a coach, but can also modify the rubrics and the model of all challenges and tasks.)
- Admin (Like an editor, but can delete users, their portfolios and their portfolio histories. Admins can also assign roles and groups to users.)
- Super admin (Like a regular admin, but can modify platform-level settings such as the authorised email domains, the platform language, and the logo. The super admin role can only be assigned by Egodact.)

(These user roles and their respective access rights are enforced by the aforementioned access rules of our databases.)

Based on the list above, it becomes clear that (super) admins pose the real risk of accidental data operations (deletion in particular) or accidental data sharing (by accidentally assigning coach, editor or admin roles to users).
While these risk will always be present due to human error, they are limited in the following ways:
- Users have to explicitly enter the admin mode before they can perform any admin operations.
- Pop-ups requesting confirmation are sent before actually deleting a user.
- Accidental role operations can easily be reversed.

Conclusion
The risks regarding privacy and personal data involved in the usage of Egodact software are relatively small. We try to reduce risks as much as we can, and even when data is breached, the risks for our users remain small.