DPIA Egodact software

26 oktober 2019, Roermond

Deze DPIA (gegevensbeschermingseffectbeoordeling) is van toepassing op de Agora VoortgangsMonitor en Agora ChallengeMonitor van Egodact (hierna: Egodact software of de/onze software).

Gegevens die verwerkt worden
De persoonsgegevens die Egodact software verwerkt zijn gering; de software verwerkt enkel de volgende persoonsgegevens van haar gebruikers (deze gebruikers zijn leerlingen en docenten in de software en zijn dus allemaal betrokkenen):

Persoonsgegeven	**Verwerking optioneel**
Volledige naam	Nee
(School) e-mailadres	Nee
Profielfoto (van het Google of Microsoft account)	Nee
Groepen waar de gebruiker in zit en/of de groepen die de gebruiker beheert (indien de gebruiker een coach is).	Ja. Groepen kunnen naar behoefte aangemaakt en toegewezen worden met beheerdersaccounts in onze software en worden niet ingesteld door Egodact.

Zoals zichtbaar zijn dit beperkte contactgegevens. Of de groepen in Egodact software überhaupt persoonsgegevens zijn valt te betwisten.

Verdere gegevens die worden opgeslagen in onze software zijn de portfolio's en portfolio geschiedenis (voortgang) van gebruikers. Met portfolio wordt hier het geheel van challenges, rijen, taken, focus, bewijs en voortgang binnen rubrics bedoeld.

Hoe deze gegevens verwerkt worden
Deze gegevens worden op twee manieren verwerkt:
- Door het gebruikersautorisatie systeem.
- Door ze op te slaan in de database.

Ze worden op meerdere plekken in onze software weergegeven, zoals terug te vinden in de privacyverklaring.

Waarom deze gegevens verwerkt worden en of deze verwerkingen noodzakelijk zijn
Alle verplichte verwerkingen van persoonsgegevens zijn noodzakelijk. Hieronder uitleg:

Persoonsgegeven	**Indien verplicht, waarom is verwerking**

	noodzakelijk?
Volledige naam	Anders kunnen gebruikers binnen onze software niet geïdentificeerd worden. Docenten moeten bijvoorbeeld via de coachmodus de portfolio's van leerlingen inzien, maar daarvoor moeten zij uiteraard wel weten van welke leerling ze het portfolio aan het inzien zijn.
(School) e-mailadres	Het e-mailadres wordt gebruikt om gebruikers te identificeren binnen het gebruikersautorisatie systeem. Verder worden portfolio's, portfolio geschiedenis en persoonsgegevens onder het e-mailadres opgeslagen in de database.
Profielfoto van het Google of Microsoft account	Dit wordt (gedeeltelijk) opgelegd door het gebruikersautorisatie systeem. Verder helpt het in de herkenning van gebruikers; het is dus ook handig.
Groepen waar de gebruiker in zit en/of de groepen die de gebruiker beheert (indien de gebruiker een coach is).	Verwerking is niet verplicht.

Verder spreekt de noodzaak van het verwerken van portfolio's en portfolio geschiedenis voor zich; dit is immers de hele functionaliteit van de software.

Verder is Egodact uiteraard GDPR compliant, zoals zichtbaar in de verwerkersovereenkomst die we met scholen afsluiten.

Opslag van gegevens

Gegevens worden op twee manieren opgeslagen (zoals benoemd in het vorige kopje):

- Persoonsgegevens worden opgeslagen in het gebruikersautorisatie systeem (Firebase Authentication) om gebruikers veilig te kunnen autoriseren.
- Alle gegevens (inclusief persoonsgegevens) worden opgeslagen in de database(s) (Firebase Real-Time Database) van Egodact software.

Zowel de database als het gebruikersautorisatie systeem maken gebruik van services van Google (Google Ireland Ltd.). Dit betekent dat gegevens worden opgeslagen in de Verenigde Staten, buiten de Europese Economische Ruimte (maar wel op een manier die GDPR compliant is aangezien Google GDPR compliant is en onder het EU-US privacy shield valt).

Bewaartermijnen en wijzigingen van gegevens

Egodact is zelf niet de "data controller" en beheert dus ook niet wanneer gegevens verwijderd worden en wanneer ze gewijzigd worden. De verantwoordelijkheid van gegevensbeheer ligt bij de school, die eigenaar blijft van de gegevens.

Wel zorgt het gebruik van Google diensten voor een vertraging van maximaal 180 dagen in het verwijderen van gegevens; Egodact kan zelf dan niet bij deze gegevens, maar Google (Firebase) kan ze wel nog opgeslagen hebben. Deze vertraging wordt ons door Google/Firebase opgelegd en wij kunnen deze niet aanpassen.

Risico's van deze gegevensverwerkingen
De risico's van deze gegevensverwerkingen zijn gering. De volgende twee risico's zijn aanwezig:

- Er doet zich een datalek voor waardoor gegevens op onrechtmatige wijze worden gedeeld met mensen die geen inzage zouden moeten hebben in deze gegevens. Ook zou een datalek tot ongewenste wijziging en verwijdering van gegevens kunnen zorgen. Dit datalek kan zowel bij Google als Egodact plaatsvinden.
- Google wordt verplicht door een (buitenlandse) overheid om gegevens te delen met een (buitenlandse) overheid.

Impact van deze risico's
Mocht een van de hierboven beschreven situaties voorkomen, is de grootte van de impact alsnog te overzien. Omdat Egodact software nauwelijks persoonsgegevens opslaat is de hoeveelheid persoonsgegevens die gelekt kan worden, en dus ook het risico voor de betrokkenen, klein. Ook zullen de gevolgen voor de vrijheden en rechten van betrokkenen erg laag zijn.

Onrechtmatige verwijdering of wijziging van gegevens vormt verder ook geen groot risico voor betrokkenen (de hoeveelheid opgeslagen persoonsgegevens is immers gering). Onrechtmatige verwijdering of wijziging van gegevens zal vooral onprettig zijn omdat de voortgang van betrokkenen verloren kan gaan.
Overigens worden persoonsgegevens hersteld naar de persoonsgegevens in het Google of Microsoft account van de betrokkene wanneer hij opnieuw inlogt in onze software.

Verder is de kans klein dat Google een verzoek krijgt om de gegevens die wij opgeslagen hebben te delen met een (buitenlandse) overheid, en zelfs als Google een dergelijk verzoek krijgt, betekent dit nog niet dat ze ingaan op dit verzoek. Google probeert naar eigen zeggen zo weinig mogelijk gegevens te delen met overheden die naar gegevens vragen.

Certificering
Google is zwaar gecertificeerd met onder andere ISO27001. Voor een gedetailleerde beschrijving van de certificaten van Google/Firebase, bekijk deze webpagina: https://firebase.google.com/support/privacy/. Verder is Google, zoals beschreven, GDPR compliant en valt Google onder het EU-US privacy shield.
Dit alles verkleint de bestaande risico's.

Hoe risico's beperkt worden
Egodact heeft geen grip op in hoeverre Google verplicht wordt gegevens te delen met (buitenlandse) overheden. Dit risico is dus niet te beperken.

Het voorkomen van datalekken—aan onze kant althans—is echter wel een risico dat we kunnen beperken. Dit doen we op de volgende manieren:

- Het zorgvuldig schrijven en updaten van de toegangsregels van onze databases. We houden beveiliging (en privacy!) altijd in ons achterhoofd bij het toevoegen van nieuwe features waardoor deze toegangsregels up to date blijven. Verder worden onze Firebase rules bij iedere versie nagelopen.
  We hebben verder weinig mogelijkheden om risico's op datalekken bij Google zelf tegen te gaan.
- Iedere school heeft haar eigen database. Verder gaan we zorgvuldig om met de wachtwoorden van de Google-accounts die we gebruiken voor de Google services; slechts enkel personen die toegang moeten hebben tot deze wachtwoorden krijgen deze toegang. Met deze personen hebben we geheimhoudingsverklaringen afgesloten of ze zijn door de wet of andere overeenkomsten met Egodact tot geheimhouding verplicht.
- We gebruiken een gebruikersautorisatie systeem om te verzekeren dat toegang tot gegevens rechtmatig wordt verkregen. (Zie het volgende kopje voor meer informatie.)

Gebruikersautorisatie en gebruikersrollen

Ten eerste: gebruikers worden altijd verplicht om in te loggen voordat ze de persoonsgegevens kunnen zien die wij hebben opgeslagen. Deze persoonsgegevens zijn nooit toegankelijk voor de buitenwereld.

Verder kent onze software de volgende gebruikersrollen:

- Leerling (Normale gebruiker; kan enkel het eigen portfolio met bijbehorende geschiedenis inzien en wijzigen.)
- Coach (Hetzelfde als een leerling, behalve dat een coach ook de portfolio's met bijbehorende geschiedenis van alle andere gebruikers kan inzien. Ook kunnen coaches binnen portfolio's van anderen feedback achterlaten en de coach sliders verplaatsen.)
- Editor (Hetzelfde als een coach, maar heeft ook nog toegang tot de editor modus. In de editor modus kunnen de rubrics die weergegeven worden in onze software aangepast worden, en kunnen de modellen (templates) van alle challenges en taken aangepast worden.)
- Admin (Een admin is een editor die ook nog toegang heeft tot de admin modus. In de admin modus kunnen gebruikers met hun portfolio's en portfolio geschiedenis verwijderd worden. Ook kunnen andere rollen worden toegewezen aan gebruikers en kunnen groepen beheerd en toegewezen worden.)
- Super admin (Kan alles wat een admin kan, maar kan verder ook nog instellingen op platform niveau wijzigen. Het gaat hier dan om instellingen zoals welke e-mailadressen gebruikt mogen worden om te in te loggen, de standaardtaal van de software en het logo dat weergegeven wordt. De super admin rol kan alleen door Egodact toegewezen worden.)

(Deze rollen met bijbehorende rechten worden afgedwongen door de eerder genoemde toegangsregels op onze databases.)

Op basis van de bovenstaande lijst wordt het duidelijk dat de grootste risico's liggen bij (super) admins. Het gaat hier dan vooral om het risico op onopzettelijke verwijdering van gegevens en het risico op het per ongeluk delen van gegevens (door het foutief toewijzen van coach, editor of admin rollen aan gebruikers).
Hoewel deze risico's altijd aanwezig zullen zijn door de menselijkheid van gebruikers (iedereen maakt immers wel eens fouten), proberen we ze op de volgende manieren wel te beperken:

- Gebruikers moeten expliciet naar de admin modus gaan voordat ze admin acties kunnen uitvoeren.
- Er worden pop-ups gestuurd die om bevestiging vragen wanneer een admin gebruikers probeert te verwijderen.
- Onopzettelijke rol wijzigingen kunnen eenvoudig teruggedraaid worden.

Conclusie
De risico's van het gebruik van Egodact software zijn met betrekking tot (persoons)gegevens dus gering. Waar we risico's zien proberen we ze te beperken, en zelfs in het geval van lekkage van (persoons)gegevens blijven de risico's voor betrokkenen klein.