DPIA Agora ChallengeMonitor

25-10-2018, 25 oktober 2018, Roermond

Inleiding
Deze DPIA (gegevensbeschermingseffectbeoordeling) is van toepassing op de Agora ChallengeMonitor van Egodact.
Deze DPIA is voor Egodact niet verplicht; gegevensverwerkingen in Agora ChallengeMonitor geven geen hoge risico's voor betrokkenen. Echter, klanten van Egodact zullen vooral scholen zijn en zij zijn wel verplicht tot het bijhouden van een DPIA. Om deze scholen tegenmoet te komen heeft Egodact alsnog een DPIA opgesteld die hieronder te vinden is.

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

Persoonsgegeven	**Verwerking optioneel**
Volledige naam	Nee
(School) e-mailadres	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 Agora ChallengeMonitor en worden niet ingesteld door Egodact.

Zoals zichtbaar zijn dit beperkte contactgegevens. Of de groepen in Agora ChallengeMonitor überhaupt persoonsgegevens zijn is afhankelijk van hoe scholen deze groepen noemen.

Verdere gegevens die worden opgeslagen in ChallengeMonitor zijn de portfolio's van gebruikers.

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

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).

Ze worden op meerdere plekken in Agora ChallengeMonitor 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 Agora ChallengeMonitor 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 en persoonsgegevens onder het e-mailadres opgeslagen in de database.
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 voor zich; dit is immers de hele functionaliteit van Agora ChallengeMonitor. Zonder deze verwerkingen zou Agora ChallengeMonitor een leeg, nutteloos platform zijn.

Ook sluiten we met scholen een verwerkersovereenkomst af waarin verdere privacyinformatie duidelijk beschreven wordt (zoals bewaartermijnen van gegevens).

Verder is Egodact uiteraard GDPR compliant, zoals zichtbaar in de privacyverklaring en verwerkersovereenkomst van de Agora ChallengeMonitor.

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 authenticeren.
- Alle gegevens (inclusief persoonsgegevens) worden opgeslagen in de database (Firebase Real-Time Database) van de Agora ChallengeMonitor.

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. Deze verantwoordelijkheid ligt bij de school, die eigenaar blijft van de gegevens.
Wel faciliteert Egodact inzage van gegevens door scholen. Wanneer Egodact een e-mail krijgt waarin een gebruiker, een betrokkene dus, vraagt om inzage van zijn gegevens, zal Egodact deze gegevens verstrekken (mits de afzender van de e-mail de rechtmatige eigenaar is van deze gegevens).

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.
- 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 Agora ChallengeMonitor 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 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 Agora ChallengeMonitor.

Verder is de kans klein dat Google een verzoek krijgt om gegevens 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.
Ook dit is een risico-verminderende factor.

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 is echter wel een risico dat we kunnen beperken. Dit doen we op twee 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.
- We koppelen iedere school met een apart Google account aan de Google services die wij gebruiken. Dit betekent ook dat iedere school zijn eigen Agora ChallengeMonitor database heeft. Deze Google accounts (alsmede admin accounts die wij vanuit scholen ontvangen) zijn beveiligd met sterke, unieke wachtwoorden (en in het geval van Google accounts ook met 2-stapsauthenticatie). Verder gaan we zorgvuldig om met wachtwoorden; 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.

Conclusie
De risico's van het gebruik van de Agora ChallengeMonitor 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.