

Whitepaper DPIA CEM

In opdracht van MBO Raad heeft ICTRecht een Data Protection Impact Assessment ('DPIA') uitgevoerd ten aanzien van de verwerkingen van persoonsgegevens door de Coöperatie Examens MBO ('CEM') in haar rol als verwerker ten opzichte van de mbo-instellingen. De CEM is een coöperatie welke digitale (reken)examens, en andere acties die op deze processen zijn gestoeld, levert aan bijna alle mbo-instellingen in Nederland. De DPIA heeft geleid tot meerdere actiepunten, waarvan enkele ook voor u als mbo-instelling van toepassing zijn.

Aan de hand van de DPIA heeft ICTRecht bekeken hoe de levering van de digitale (reken)examens, en andere acties die op deze processen zijn gestoeld, te werk gaat, welke gegevens er worden verwerkt en welke privacyrisico's er eventueel zijn. De risico's zijn geconstateerd ten aanzien van de mbo-instelling als verwerkingsverantwoordelijke, maar ook ten aanzien van de CEM als verwerker en ten opzichte van haar leveranciers als subverwerkers.

De digitale (reken)examens worden afgenomen en ontwikkeld middels het digitale examenplatform Remindo (MBO) en MijnRekenPortfolio/Skillsy (Entree) van Paragin. De afname van de examens en de metingen vinden plaats onder verantwoording van de mbo-instellingen. Voor psychometrische analyses (anonieme gegevens) werkt de CEM samen met Cito. Voor het inplannen van beoordelaars voor de examens gebruikt de CEM de Beoordelaarsmodule van Stipp. Door middel van de software van Paragin en Stipp worden veel persoonsgegevens verwerkt. Dat betekent dat de privacywetgeving (Algemene verordening gegevensbescherming/AVG) van toepassing is.

Op basis van de risico's en aandachtspunten die in de DPIA zijn vastgesteld is een actielijst opgesteld. Hieronder volgt een opsomming van die acties. De actielijst bevat concrete acties die door de mbo-instellingen opgepakt dienen te worden. Daarnaast staan hierin ook enkele aandachtspunten die meegenomen dienen te worden bij het opstellen van beleid. Dit om ervoor te zorgen dat privacy wordt gewaarborgd.

Actiepunten:

- **Specificeren partijen en betrokkenen:** de mbo-instelling dient het overzicht van persoonsgegevens en betrokken partijen bij te werken indien er (categorieën van) persoonsgegevens of partijen worden toegevoegd of verwijderd.
- **Doelbinding:** de mbo-instelling dient de verwerkingsdoeleinden van verwerkingen door de CEM vooraf vast te stellen en vast te leggen in het verwerkingsregister.
- **Opslagbeperking:** de mbo-instelling dient bewaartermijnen vast te stellen en vast te leggen. De mbo-instelling is zelf verantwoordelijk voor de verwijdering van (automatisch) bewaarde persoonsgegevens. Wij adviseren de mbo-instelling om de verwijdering van reeds vastgestelde termijnen in te voeren.
- **Afspraken met derde partijen:** de mbo-instelling dient een verwerkersovereenkomst te sluiten met de CEM.
- **Informereren:** de mbo-instelling dient betrokkenen te informeren over de verwerking van hun persoonsgegevens. Dit dient zij te doen door een privacyverklaring voor studenten en een interne privacyverklaring voor medewerkers beschikbaar te stellen.

- **Aantoonbaarheid:** de mbo-instelling dient het verwerkingsregister bij te werken met alle verwerkingen die worden uitgevoerd door de CEM. Daarbij dient onder andere te worden uitgelegd welke persoonsgegevens van studenten en medewerkers verstrekt worden aan Paragin en Stipp, hoelang de gegevens bewaard blijven en welke beveiligingsmaatregelen zijn getroffen.