Burgemeester Jamessingel 2
2803 PD GOUDA
KvK 81749481
info@gouwe-academie.nl
www.gouwe-academie.nl

Gouwe Academie onderwerpt instrument Zien! aan DPIA

Gouwe Academie neemt de privacywetgeving serieus en daarom hebben we aan de leverancierszijde een DPIA uitgevoerd. DPIA staat voor *Data Protection Impact Assessment,* ook wel gegevensbeschermingseffectbeoordeling genoemd. De verantwoordelijkheid bij het afnemen van een DPIA ligt bij de verwerkingsverantwoordelijke (in de praktijk vaak een school(bestuur)). Bij Gouwe Academie vinden we het belangrijk dat onze instrumenten ook op AVG-vlak betrouwbaar zijn, en daarom hebben we ook aan de leverancierszijde een DPIA uitgevoerd voor het instrument Zien!. Dit is noodzakelijk omdat er bij Zien! sprake is van gegevens die gaan over de gezondheid (namelijk: het welzijn) van een kind. Daarnaast is er sprake van gegevensverzameling en stelselmatige monitoring van kwetsbare betrokkenen.
Gebruikers van Zien! kunnen de door Gouwe Academie uitgevoerde DPIA als basis gebruiken voor hun eigen uit te voeren DPIA, en daarmee is dit document een vorm van dienstverlening die we beschikbaar stellen aan onze klanten. In dit bericht vertellen we kort iets over het proces en de belangrijkste adviezen die uit de DPIA volgen.

Het werkproces

Allereerst hebben we nagedacht over de vraag óf en zo ja met welke personen we een DPIA moeten uitvoeren. Omdat er sprake is van dataverwerking van een kwetsbare doelgroep (namelijk leerlingen) is het noodzakelijk om een DPIA uit te voeren. Een aantal collega's van Gouwe Academie (manager, beleidsmedewerker, onderwijsadviseurs en AVG-specialist), collega's van onze technische partner Educator (manager en ontwikkelaar) én collega's uit het veld hebben gezamenlijk nagedacht over mogelijke AVG-risico's aan de hand van de MAPGOOD-methode. Middels deze methode is het mogelijk om op stelselmatige wijze te onderzoeken of en welke risico's zich mogelijk voordoen op specifieke categorieën bij het gebruik van een softwareproduct. We hebben deze risico's geformuleerd vanuit het oogpunt van de beheerder op een school of samenwerkingsverband. Op basis van dit werkproces zijn een aantal potentiële risico's gesignaleerd in het gebruik van Zien!. Deze risico's zijn ieder ingeschaald op een schaal van 1 (weinig risico) tot 9 (veel risico). De punten met het hoogste risico zijn hieronder benoemd. Daarnaast worden adviezen voor de verwerkingsverantwoordelijken aan deze risico's gekoppeld om de risico's op te heffen of sterk te verminderen.

Adviezen

In de tabel hieronder vind je de categorie en dreiging, gecategoriseerd volgens de MAPGOOD-methode. In de samenvatting van deze MAPGOOD-methode worden de adviezen geschreven. In de linkerkolom is zichtbaar uit welke MAPGOOD-categorie dit komt. In de middelste kolom is zichtbaar welke risicoscore de dreiging betreft. In de rechterkolom wordt het advies beschreven.

Categorie – dreiging (MAPGOOD)	**Risico 1 (weinig) – 9 (veel)**	**Adviezen**
Mens-wegvallen: voorzienbaar (ontslag, vakantie)	2	Stel minimaal twee mensen aan als applicatiebeheerder. Dit zijn ook de mensen die aanspraak kunnen maken op contacten met de helpdesk. Beheerders kunnen straks inzien welke accounts een jaar (of langer) niet zijn gebruikt. Intentie-uitspraak is dat we de ontwikkeling hiervan in zomer '23 opstarten. Deze accounts kunnen door de beheerder worden dichtgezet. Bovendien zou vertrek van een collega altijd moeten worden doorgegeven aan een beheerder.
Mens-opzettelijk menselijk handelen: fraude, diefstal, lekken van informatie	2	Publiceer zo min mogelijk mailadressen van collega's die Zien! gebruiken op een openbare, online plek. Maak, bij het weergeven van contactmogelijkheden voor collega's, gebruik van contactformulieren of gebruik een verwijzing naar LinkedIn of een "klik hier" knop.

Programmatuur-nalatig handelen: slechte documentatie	2	Zorg dat documentatie, waaronder de handleiding, altijd up-to-date is. Doe deze check bij voorkeur vier keer per jaar. Daarnaast is het aan te bevelen dat de beheerder altijd kennisneemt van de nieuwste ontwikkelingen. Deze staan onder Informatief en worden gedeeld via de nieuwsbrief. Tot slot is het omtrent dit punt belangrijk dat data-bewaartermijnen worden gehandhaafd: pas AVG-wetgeving en functionaliteit toe. De verwerkingsverantwoordelijke is hiervoor verantwoordelijk.
Gegevens-via gegevensdragers: diefstal, zoekraken, lekken	4	Laat geen gegevensdragers achter waar privacygevoelige data op staat. Denk aan USB-sticks en geprinte bestanden. Daarnaast kan gedacht worden aan lokale bestanden in de map downloads: stel daarvoor bijvoorbeeld via accountbeheer in dat de map downloads automatisch wordt geleegd met een bepaald tijdsinterval. Denk tot slot aan het afmelden van de laptop als er geen gebruik van wordt gemaakt (en niet slechts dichtklappen) of afmelden in de browser (en niet slechts de browser afsluiten).
Gegevens-via gegevensdragers: foutieve of geen versleuteling	4	Maak gebruik van multi factor authenticatie (MFA). Voor Zien! is de intentie dat we medio zomer 2023 met deze ontwikkeling starten.
Gegevens-via cloudvoorziening en: ongeautoriseerde toegang door onbevoegden (hackers/hosters)	3	Regel met de ICT-provider dat er altijd een up-to-date firewall aanwezig en geïnstalleerd is. Zorg voor bewustzijn bij collega's hoe een poging tot hacking/phishing herkend kan worden (vast onderdeel van technische scholing/opleiding voor nieuwe gebruikers, zie onderdeel *organisatie-gebruiksorganisatie: gebrekkige toedeling taken, bevoegdheden en verantwoordelijkheden*).
Organisatie-gebruiksorganisatie: gebrekkige toedeling taken, bevoegdheden en verantwoordelijkheden	4	Zorg dat beheerders voldoende zijn opgeleid om te voorkomen dat verkeerde rollen en rechten worden toegekend. Hiertoe verzorgt Gouwe Academie verplichte technische scholingen (Zien!vo). Middels deze verplichte technische scholingen wordt een certificaat behaald , passend bij de implementatiefase waar de school in zit.

Tot slot

Hierboven heb je meer kunnen lezen over de DPIA Zien! van Gouwe Academie en de adviezen die daaruit voortgekomen zijn. Je kunt deze adviezen gebruiken om je eigen DPIA op jouw school vorm te geven. Heb je behoefte aan meer informatie of wil je het volledige DPIA-rapport ontvangen? Dat kan. Stuur een mail naar helpdeskzien@gouwe-academie.nl Eén van onze collega's helpt je dan verder.