Gouwe Academie voert DPIA uit voor Kindkans

Gouwe Academie neemt de privacywetgeving serieus! 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)). Wij van Gouwe Academie vinden 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 Kindkans. Dit is noodzakelijk omdat er bij Kindkans sprake is van gegevens die gaan over de gezondheid (namelijk: het welzijn) van een kind. Daarnaast wordt dit instrument gebruikt binnen een samenwerkingsverband. Tot slot er is er sprake van gegevensverzameling en stelselmatige monitoring van kwetsbare betrokkenen.
Gebruikers van Kindkans 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 deze samenvatting de DPIA vertellen we kort iets over het proces wat we met elkaar doorlopen hebben en de belangrijkste adviezen die uit de DPIA volgen.

Het werkproces

Allereerst hebben we met elkaar nagedacht over de vraag óf en zo ja met welke personen we een DPIA 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, onderwijsadviseur 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 Kindkans. 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 verwerkingsverantwoordelijke 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 linker kolom 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)**	**Advies**
Mens-wegvallen: voorzienbaar (ontslag, vakantie)	4	Stel een hoofdbeheerder aan in een beheerdersrol. Deze kan aanspraak maken op contacten met de helpdesk. Zorg hiernaast voor een schaduwbeheerder, die dit kan waarnemen of overnemen. Beheerders kunnen inzien welke accounts een jaar (of langer) niet zijn gebruikt. Deze accounts kunnen door de beheerder worden gedeactiveerd. Bovendien moet vertrek van een collega worden doorgegeven aan een beheerder.
Mens-opzettelijk menselijk handelen: fraude, diefstal, lekken van informatie	3	Publiceer zo min mogelijk mailadressen van collega's die Kindkans 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	4	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 de releasenotes van nieuwe versies tot zich neemt. Tot slot is het omtrent dit punt belangrijk dat data-bewaartermijnen worden gehandhaafd: pas AVG-wetgeving en functionaliteit toe. De verwerkingsverantwoordelijke is hiervoor verantwoordelijk.
Apparatuur-opzettelijk menselijk handelen: (ongeautoriseerde) functieverandering en/of toevoeging	4	Zorg dat beheerders voldoende zijn opgeleid om te voorkomen dat verkeerde rollen en rechten worden toegekend. Hiertoe faciliteert Gouwe Academie in (sterk aanbevolen) klankbordbijeenkomsten en een certificaat of opleiding voor nieuwe Kindkansgebruikers. Daarnaast blijven we werken met een strippenkaart om klanten zo goed mogelijk te helpen via de helpdesk.
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 Kindkans is dit reeds beschikbaar.
Gegevens-via cloudvoorzieningen: ongeautoriseerde toegang door onbevoegden (hackers/hosters)	3	Regel met 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 opleidings- en certificeringsproces, zie onderdeel *apparatuur-opzettelijk menselijk handelen ((ongeautoriseerde) functieverandering en/of toevoeging*).
Gegevens-via apparatuur: onvoldoende toegangsbeperking tot apparatuur	6	Zie advies bij onderdeel *apparatuur-opzettelijk menselijk handelen ((ongeautoriseerde) functieverandering en/of toevoeging*.
Organisatie-gebruiksorganisatie: gebrekkige toedeling taken, bevoegdheden en verantwoordelijkheden	4	Zie advies bij onderdeel *apparatuur-opzettelijk menselijk handelen ((ongeautoriseerde) functieverandering en/of toevoeging*.
Organisatie-gebruiksorganisatie: onduidelijke of ontbrekende gedragscodes	4	Zorg voor een duidelijke gedragscode die voldoet aan AVG-normen. Deel bijvoorbeeld als beheerder iets met IB'ers hoe Kindkans werkt en laat frequent aandachtspunten aan bod komen.

Tot slot

Hierboven heb je meer kunnen lezen over de DPIA Kindkans van Gouwe Academie en de adviezen de daaruit voortgekomen zijn. Je kunt deze adviezen gebruiken om je eigen DPIA op jouw school vorm te geven.