Update rapportage verbetermaatregelen DPIA Somtoday – Topicus
versie 1.3, oktober 2022

Inleiding

In 2021 in een DPIA (Rapportage DPIA - Somtoday v1.1) uitgevoerd op het leerlingadministratiesysteem Somtoday. In de DPIA wordt aanbevolen om risico-beperkende beheersmaatregelen uit te voeren om de aangetroffen privacyrisico's te beperken. De mitigerende maatregelen bestaan uit organisatorische maatregelen bij de school, maatregelen m.b.t. de inrichting van de dienst en tot slot maatregelen vanuit de leverancier van de dienst. Dit document beschrijft een update van de genomen en te nemen maatregelen van Somtoday – leverancier Topicus - om de benoemde risico's in de DPIA te mitigeren. In het DPIA rapport van 2021 is de reactie van Somtoday niet verwerkt. Het kan dus zijn dat de constateringen op de datum van publicatie van de DPIA reeds niet meer van toepassing waren.

SIVON is voornemens om de uitgevoerde DPIA's op de leerlingadministratiesystemen te herhalen. Hierbij wordt de systematiek gevolgd van de DPIA's op de systemen van Microsoft, Google en personeelsadministratiesystemen. De uitkomsten van de eerdere DPIA worden daarin meegenomen.

Hoe is onderstaande tabel tot stand gekomen

In het Somtoday DPIA rapport zijn een set maatregelen benoemd om de risico's te beperken. De maatregelen die de leverancier (=verwerker) genomen heeft staan in onderstaande tabel. In de kolom "maatregel verwerker" staan de maatregelen van Somtoday. De kolom "status" geeft aan of deze maatregel voldoende is. Deze kolom is tot stand gekomen in samenwerking met schoolbesturen.

Conclusie

Een aantal van de constateerde hoge risico's zijn door de leverancier gemitigeerd, een aantal risico's moeten door het schoolbestuur worden beperkt door het nemen van (aanvullende) organisatorische maatregelen.

Risico nummer	Risico	Risico waardering	Risicobeschrijving	Maatregel verwerker	Status
5.4.1	Er zijn passende maatregelen genomen om de continuïteit van het onderwijs te waarborgen (AVG art. 32)	Hoog	Er is een op actuele risico's afgestemde procedure om in het geval van DDOS aanvallen de continuïteit te borgen.	Sinds 16 april 2021 is Somtoday tegen DDoS-aanvallen beschermd met behulp van de Cloudflare web application firewall. Sindsdien zijn alle DDoS-aanvallen succesvol afgeslagen en hebben niet geleid tot productiestoringen	Met de benoemde maatregelen van de leverancier resteert er geen restrisico.
5.5.2	Bijzondere of gevoelige persoonsgegevens worden beveiligd gemaild (AVG art. 32).	Zeer Hoog	Persoonsgegevens kunnen vanuit het LAS worden uitgewisseld via een mailvoorziening of toepassing voor interne berichten die voldoet aan de standaarden en conventies voor beveiligd mailen (NTA7516 en/of 'UBV Veilig en Betrouwbaar e-mailverkeer'). Het mailen naar grote groepen wordt beperkt en/of er zijn extra controle mechanisme die voorkomen dat mails naar de verkeerde ontvangers worden gestuurd.	NTA 7516 is een norm voor de medische sector. Deze norm laat zich niet eenzijdig implementeren: zowel de partij die de mail verstuurt als de ontvanger moet deze norm implementeren. De mailvoorziening van Somtoday voldoet aan de richtlijnen UBV Veilig en Betrouwbaar e-mailverkeer (anti-phishing conform SPF, DKIM en DMARC, beveiligen mailserver met TLS).	De leverancier voldoet aan de richtlijnen UBV Veilig en Betrouwbaar mailverkeer. Aan het versturen van persoonsgegevens per e-mail blijven privacy-risico's kleven. Het bevoegd gezag kan in het interne beleid van het schoolbestuur vastleggen of en op welke wijze gebruik mag worden gemaakt van de mailvoorziening. Gebruikers moeten hiertoe aparte instructies krijgen. Indien persoonsgegevens niet via de mail verzonden mogen worden is er een laag restrisico, bij een beleid rondom gebruik van de interne mailvoorziening en een bijbehorende gebruiksinstructie een gemiddeld privacy-risico.
5.5.3	Het maken van handmatige	Hoog	Persoonsgegevens worden vanuit het LAS/LVS uitgewisseld via	In het Somtoday Connect applicatie-overzicht vind je het aanbod van alle	Niet alle applicaties kunnen rechtstreeks gekoppeld worden via

	exports van persoonsgegevens is niet toegestaan, zonder voldoende waarborgen voor de bescherming van de persoonsgegevens (AVG art. 32).		beveiligde geautomatiseerde koppelingen. Het werken met handmatige exports is alleen beargumenteerd toegestaan met expliciete toestemming van de verwerkingsverantwoordelijke (het bevoegd gezag). Er wordt centraal (vanuit beheer) controle op (logging van) exports uitgevoerd.	type applicaties die je veilig kunt koppelen met Somtoday. Je vindt hier alleen applicaties die voldoen aan de privacywetgeving. Somtoday legt in haar partnerovereenkomst vast dat de partner een verwerkerovereenkomst sluit met de school. Om de correcte uitvoering te borgen biedt Somtoday scholen die Connect afnemen een verplichte training aan over de inrichting en bediening van Connect. Handmatige exports vanuit Somtoday kennen meer toepassingen in de dagelijkse praktijk op scholen. Exports worden bijvoorbeeld gebruikt om gegevens nader te analyseren in Excel of om uit te printen. Het recht om handmatig exports uit te voeren kan per rol of op individuele basis worden toegekend.	Connect. Data minimalisatie is niet mogelijk via de standaard Connect koppeling. School maakt (nog) geen gebruik van de betaalde versie waarin het mogelijk is de aangeboden data per aangesloten leverancier in te stellen (er is een beperkt aantal leveranciers aangesloten). Er is geen rest-risico als de aanvullende module is geïmplementeerd. Handmatige exports zijn nog steeds een hoog risico, diverse geautoriseerde medewerkers kunnen exports maken. Dit wordt wel beperkt door autorisatie, er wordt niet gemonitord op welke gegevens door wie worden geëxporteerd. Inventariseer of het interne beleid dit risico voldoende adresseert en daarmee mitigeert. Gedragsregels en afspraken beperken het risico van handmatige exports gedeeltelijk tot een laag risico.
5.5.4	De bescherming van de juistheid en de consistentie van persoonsgegevens wordt	Midden	De wijzigingen die door ouders/verzorgers en leerlingen worden ingevoerd in het LAS, kunnen gevalideerd en goedgekeurd worden door de school.	Scholen kunnen ouders/verzorgers en leerlingen in staat stellen om hun contactgegevens te wijzigen (mail, mobiel). Somtoday kan hier in overleg met scholen een extra validatieslag aan toevoegen	Scholen moeten contact opnemen met de leverancier om een extra validatieslag toe te voegen. Zonder deze validatie blijft het risico aanwezig (midden).

	gewaarborgd. (AVG art. 5, 32).				Ouders kunnen via het ouderportaal, zonder controle, school- mail- en telefoongegevens wijzigen, de gegevens worden automatisch ook in Somtoday verwerkt.
5.5.5	Er mogen niet meer persoonsgegevens worden uitgewisseld dan strikt noodzakelijk en alleen op basis van grondslag en doelbinding (AVG art. 5, 6, 25).	Laag	Geautomatiseerde koppelingen kunnen in het LAS door of op verzoek van het schoolbestuur ingezien en zo nodig gewijzigd worden op basis van noodzakelijkheid, grondslag en doelbinding	Dit is precies waar de nieuwe AVG-module van Somtoday Connect zich op richt. Met het Somtoday connect dashboard zie je met welke applicaties je allemaal koppelt en is het mogelijk om zelf koppelingen tot stand te brengen en alleen die data te delen die nodig is. https://som.today/modules/connect-2/inzicht-plus/	Somtoday Connect is opgenomen in een aparte module waarvoor extra betaald moet worden. Het is dus alleen mogelijk om data minimalisatie toe te passen als deze (extra) module wordt afgenomen door de school. Zie ook 5.5.3. Bij implementatie van deze module resteert er geen restrisico.