

Privacy is de randvoorwaarde voor het gebruik van Google Workspace for Education

In augustus 2021 publiceerde SIVON de stappen die scholen moeten zetten om Google Workspace for Education te kunnen blijven gebruiken [<https://www.sivon.nl/actueel/google-workspace-for-education-blijven-gebruiken-voer-eerst-deze-handelingen-uit/>]. De afgelopen periode heeft SIVON veel vragen gekregen over de gevolgen van de technische instellingen die scholen moeten gebruiken. Hierdoor kunnen onderdelen van Workspace for Education namelijk niet of anders worden gebruikt. In dit artikel leggen we kort uit waarom het belangrijk is dat u deze instellingen wel aanpast, hoe de afspraken met Google tot stand zijn gekomen en hoe we u kunnen ondersteunen bij de technische instellingen.

Privacy is een recht

In het onderwijs maken we steeds meer gebruik van persoonsgegevens en ict. We slaan steeds meer informatie op en wisselen digitaal steeds meer informatie uit. Dit doen niet alleen scholen, maar ook de leveranciers van digitale leermiddelen. Leerlingen, ouders en medewerkers willen erop kunnen vertrouwen dat scholen correct met hun gegevens omgaan en de privacy waarborgen.

Bij het gebruik van Google Workspace for Education gaat het steeds over privacy. Privacy is enerzijds het recht om met rust te worden gelaten. Anderzijds gaat het over het recht om gegevens over jezelf te kunnen controleren. Als je weet dat je bij alles wat je doet gevolgd wordt én dat dit gevolgen voor jou kan hebben, dan pas je jouw gedrag daarop aan. Zonder het recht op privacy kan een mens niet vrij zijn. Privacy is een randvoorwaarde in een democratische samenleving. Daarom blijft het belangrijk dat scholen privacy goed organiseren.

Start onderzoek naar privacyrisico's

In 2020 is begonnen met een onderzoek naar de privacyrisico's van het gebruik van Google Workspace for Education (voorheen was dit G-Suite for Education). Dit onderzoek is een Data Protection Impact Assessment (DPIA, ook wel gegevensbeschermingseffectbeoordeling), waarbij wordt onderzocht of de persoonsgegevens voldoende beschermd zijn. Deze DPIA is gestart door de Hogeschool van Amsterdam en de Rijksuniversiteit Groningen. Omdat er in het onderwijs in alle sectoren in meer en mindere mate gebruik wordt gemaakt van Google Workspace for Education, hebben SURF en SIVON namens de gehele onderwijssector zich aangesloten bij dit onderzoek. Daarbij worden we ondersteund door de Privacy Company die de DPIA uitvoert, SLM Rijk (ministerie van Justitie en Veiligheid) en GT Law bij de onderhandelingen met Google. Hierbij is intensief overleg en afstemming geweest met het ministerie van Onderwijs, Cultuur en Wetenschap en de sector- en koepelorganisaties.

Uitkomst: hoge privacyrisico's die moeten worden aangepakt

De [uitkomsten van de eerste DPIA](#) van maart 2021 laten zien dat het gebruik van Google Workspace for Education niet zonder risico is. Het gaat om de volgende hoge privacyrisico's:

- a. Geen duidelijke rolverdeling voor metadata: bij het gebruik van Google Workspace for Education blijven scholen wel eigenaar van de gegevensbestanden van de gebruikers (denk aan Google Docs, Presentation, Sheets, Calendar en Gmail). Maar bij het gebruik van de Google-producten houdt Google ook informatie bij over hoe gebruikers Google gebruiken. Bijvoorbeeld het tijdstip van inloggen en hoe lang de producten worden gebruikt. We noemen dit metadata. Scholen kunnen hierover geen goede afspraken met Google maken, waardoor zij hun rol al verwerkingsverantwoordelijke niet of onvoldoende waar kunnen maken.
- b. Onvoldoende controle over de doelen waarvoor Google gegevens verzamelt en mag gebruiken.

- c. Google is onvoldoende transparant over welke gegevens ze verzamelt en wat ze met die gegevens doet.
- d. Google en de school hebben vanwege het gebrek aan de juiste privacyafspraken geen juridische grond om Google Workspace for Education te gebruiken, daarmee handelen ze in strijd met de grondbeginselen van de AVG.
- e. Er is onvoldoende toezicht en controle op de verwerking van persoonsgegevens door Google, scholen hebben onvoldoende middelen om gegevens te controleren.
- f. Er is onvoldoende bekend over de afspraken die Google heeft gemaakt met haar toeleveranciers, subverwerkers genoemd.
- g. Gebruikers worden onvoldoende geïnformeerd over wat Google met hun gegevens doet en gebruikers kunnen hun privacyrechten onvoldoende uitoefenen, zoals het recht op inzage.

Nieuwe afspraken om privacyrisico's te beperken

De privacytoezichthouder, de Autoriteit Persoonsgegevens, [stelde eind mei 2021 vast](#) dat al deze hoge privacyrisico's zo ernstig zijn dat scholen geen gebruik meer mogen maken van Google Workspace for Education. Doordat scholen onvoldoende controle houden op de gegevens die Google verwerkt, komt de privacy van (veelal minderjarige) leerlingen, studenten en medewerkers ernstig in gevaar. Scholen handelen hiermee in strijd met de wet en kunnen een boete krijgen en reputatieschade oplopen. Het gebruik van Google Workspace for Education moest daarom worden stopgezet, tenzij SURF en SIVON nieuwe privacyafspraken zouden maken met Google. En dat is gelukt. De uitkomst leest u in [dit bericht](#). Als al deze nieuwe afspraken worden nagekomen, zijn de hoge risico's beperkt. Scholen kunnen dan Google blijven gebruiken. Ze houden dan de controle over de persoonsgegevens en privacy van hun leerlingen en medewerkers.

Technische instellingen voor veilig gebruik

Ondanks de nieuwe afspraken met Google blijft het veilig gebruiken van Google Workspace for Education complex. Dit komt omdat er geen duidelijke grens is tussen de zakelijke en consumenten diensten van Google. De overeenkomst met Google gaat over de core Workspace-diensten, denk aan Google Docs, Gmail en Google Drive. Deze diensten zijn vaak verweven met diensten die niet onder de overeenkomst vallen, denk aan spellingcheck, Google Search en Google Maps. Deze laatstgenoemde diensten vallen nog onder de online terms of service, waarbij Google verwerkingsverantwoordelijke is voor de persoonsgegevens die ontstaan bij het gebruik van deze diensten. Als schoolbestuur heeft u geen grip op wat Google met de gegevens doet die ze via deze diensten verzamelt. Daarom leggen de technische instellingen die onderdeel zijn van de nieuwe afspraken beperkingen op in het gebruik van deze diensten. Zonder de technische instellingen blijven de hoge privacyrisico's bestaan en is het gebruik van de diensten in strijd met de AVG, en dus niet toegestaan.

Denk vooraf goed na over privacy zodat het geen belemmering wordt

“Als u vooraf goed nadenkt over de rol van informatiebeveiliging en privacy binnen uw school, hoeft privacy geen belemmering te zijn om probleemloos gebruik te maken van ict”, zegt Job Vos, senior adviseur privacy bij SIVON. “Het veilig en verantwoord gebruik van persoonsgegevens is een randvoorwaarde voor het probleemloos gebruik van ict in het onderwijs.”

Een DPIA is een goed hulpmiddel om de gevolgen in te schatten voor de privacy van de gebruikers van nieuwe software. Door op tijd met een DPIA te beginnen, weet u vooraf welke maatregelen u moet nemen om de privacyrisico's te beperken. Dat voorkomt achteraf veel problemen.

Ondersteuning bij privacy

Privacy goed regelen is complexe materie. Het vereist goede kennis van ict-systemen en wetgeving. Inzicht in ict is nodig om te doorzien welke data op welke manier verwerkt worden om vervolgens te kunnen beoordelen of ze voldoen aan de wet- en regelgeving. We kunnen ons voorstellen dat u hier ondersteuning bij nodig heeft. Er zijn verschillende bedrijven die u hierbij kunnen helpen.

Om scholen te helpen bij het regelen van IBP heeft Kennisnet in samenwerking met de PO-Raad en VO-raad een stappenplan ontwikkeld; [de Aanpak IBP](#). De aanpak IBP sluit aan bij wet- en regelgeving en internationale normen voor informatiebeveiliging, zoals ISO 27001. Vooraf goed nadenken wat de gevolgen kunnen zijn voor de privacy van leerlingen en medewerkers zorgt ervoor dat u niet overvallen wordt door problemen bij uw leverancier. Daarnaast kunnen privacy- en beveiligingsfunctionarissen en functionarissen voor gegevensbescherming zich aansluiten bij [het Netwerk IBP po/vo](#) van de PO-Raad, VO-raad, Kennisnet en SIVON. Hier worden ervaringen en best practices uitgewisseld tussen scholen en er wordt kennis gedeeld over actuele ontwikkelingen rondom IBP.

Verder zijn er [gespecialiseerde bedrijven](#) actief voor het onderwijs om te helpen met het organiseren van privacy. Een aantal van hen biedt specifiek ondersteuning bij het uitvoeren van DPIA's en de problemen rondom Google.