DPIA's Microsoft

In opdracht van de overheid heeft Privacy Company de afgelopen jaren verschillende DPIA's uitgevoerd op een aantal Microsoft-producten. De uitkomsten van die DPIA's hebben geleid tot een aantal aanbevelingen.[1]

Er zijn dus goede stappen gezet om te zorgen dat overheidsorganisaties en onderwijsinstellingen volgens de regels van de AVG met Microsoft-producten en -diensten kunnen werken. Het gaat dan om de producten en diensten die onderwijsinstellingen via SURF, APS IT-diensten of SLBdiensten hebben aangeschaft.

Van onderwijsinstellingen is echter ook nog actie vereist om de deze producten en diensten echt AVG-compliant te maken. Dit doen zij door de onderstaande aanbevelingen van Privacy Company zo snel mogelijk door te voeren. Bij vragen over de technische maatregelen kunnen zij het beste contact opnemen met hun leverancier.

Hieronder staan de maatregelen per product opgenoemd. Bij maatregelen die organisatorisch van aard zijn, is dat erachter vermeld.

Aanbevelingen DPIA Windows 10

- Stel de telemetrie op het laagste niveau 'Beveiliging' in of blokkeer de telemetrie
- Blokkeer centraal de Windows Tijdlijn.

Aanbevelingen DPIA Office 365 ProPlus versie 1905

- Blokkeer centraal het gebruik van de (optionele) Controller Connected Experiences[2]
- Upgrade naar versie 1905 of hoger van Office 365 ProPlus
- Schakel het Customer Experience Improvement Programma (CEIP) uit
- Zet LinkedIn integratie uit voor Microsoft werknemer accounts

[1] Meer (achtergrond)informatie over deze aanbevelingen is te vinden in de (samenvattingen van de) DPIA's:
DPIA's uit 2019: https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise.
DPIA's uit 2020: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps en https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-intune.
Zie voor meer informatie ook de blogs van Privacy Company: https://www.privacycompany.eu/blogpost-nl/onderzoek-naar-microsoft-office-365-for-the-web-en-apps-microsoft-belooft-nieuwe-maatregelen-om-hoge-privacyrisicos-te-verlagen.

[2] Ten tijde van de DPIA ging het om 14 optionele Controller Connected Experiences, maar Microsoft heeft zich het recht voorbehouden om hier wijzigingen in aan te brengen. Het actuele overzicht daarvan is terug te vinden op: https://docs.microsoft.com/en-us/deployoffice/privacy/optional-connected-experiences.

Aanbevelingen DPIA's Office 365 ProPlus en Office Online en mobiele Office apps

- Functies zoals Workplace Analytics, MyAnalytics, Delve en Activity Reports in het Microsoft 365 admin center staan standaard aan. Zet deze functies allemaal uit en voer eerst DPIA's uit voordat wordt besloten om deze functies afhankelijk van de uitkomst van de DPIA in gebruik te nemen. Voor het onderwijs geldt deze aanbeveling ook voor Insights. |*technisch én organisatorisch*
- Voer DPIA's uit voorafgaand aan het gebruik van Workplace Analytics and Activity Reports in het Microsoft 365 admin center en voordat werknemers gebruik kunnen maken van MyAnalytics and Delve. Voor het onderwijs geldt deze aanbeveling ook voor Insights. | *organisatorisch*
- Overweeg gebruik van Customer Lockbox en Customer Key, afhankelijk van de gevoeligheid van de inhoudelijke gegevens.[3] | *organisatorisch*

Aanbevelingen DPIA's Office for the Web (Office Online) en mobiele Office apps (zolang Microsoft nog niet de beloofde maatregelen heeft genomen)[4]

- Stel beleid op om werknemers te waarschuwen dat zij de mobiele Office apps niet mogen gebruiken, dan wel maak de afweging of de mobiele Office apps centraal geblokkeerd moeten worden voor het zakelijke Office-account. | *organisatorisch*
- Stel beleid op om werknemers te waarschuwen dat zij de Controller Connected Experiences in Office for the Web/Online-applicaties niet mogen gebruiken. | *organisatorisch*

Aanbevelingen DPIA's Office for the Web (Office Online) en mobiele Office apps (nadat Microsoft de toegezegde maatregelen heeft doorgevoerd)

- Schakel de Controller Connected Experiences uit
- Zet de telemetrieverzameling in de mobiele Office apps op het laagste niveau

[3] Hier kunnen (extra) kosten aan verbonden zijn.

[4] De verschillende maatregelen zouden door Microsoft in het vierde kwartaal van 2020 moeten worden doorgevoerd. Hou hiervoor de berichtgeving van SLM Rijk in de gaten.

- Gebruik als beheerder regelmatig de Data Viewer Tool om de telemetrie te bekijken die vanuit de mobiele Office-apps wordt verzonden
- Maak in de eigen organisatie bewaartermijnenbeleid bekend en dwing naleving af / ruim verouderde gegevens op vanwege de risico's van doorgifte naar de VS. | *organisatorisch*
- Informeer werknemers en leerlingen over hun recht op inzage van de diagnostische gegevens die Microsoft verzamelt via de DSR en de audit logbestanden. | *organisatorisch*

Aanbevelingen om de resterende lage gegevensbeschermingsrisico's van het gebruik van Office for the Web/ Online en mobiele Office apps voor zover mogelijk te mitigeren

- Actualiseer je verwerkingsregisters en het bestaande privacybeleid voor werknemers met specifieke informatie voor welke doelen en onder welke omstandigheden de organisatie de verschillende soorten diagnostische gegevens uit Microsofts verschillende diensten en producten mag bekijken. | *organisatorisch*
- Volg de adviezen van SLM Microsoft Rijk over de jurisprudentie van het Hof van Justitie EU over de doorgifte van persoonsgegevens naar de Verenigde Staten. | *organisatorisch*

De overheid heeft in 2019 ter ondersteuning bij de aanbevelingen een factsheet 'AVG compliant gebruikmaken van Microsoft Windows 10 Enterprise en Office ProPlus' gepubliceerd.[5] Ook de Microsoft-leveranciers voor het primair en voortgezet onderwijs hebben hun klanten in juli 2020 een handleiding gestuurd waarin wordt uitgelegd hoe een aantal van de bovenstaande technische maatregelen kunnen worden uitgevoerd.

Let op bij geïntegreerde apps!

Geïntegreerde apps (bijvoorbeeld in Teams) zijn meestal producten van een andere leverancier en vallen niet onder de Microsoftvoorwaarden. Controleer dus goed de voorwaarden van de betreffende app en leverancier voordat je met een dergelijke app gaat werken.

[5] https://slmmicrosoftrijk.nl/wp-content/uploads/2019/08/Factsheet-AVG-compliant-gebruik-Windows10-en-Office-ProPlus-20190815.pdf