Checklist verwerkersovereenkomst (onderwijs)

Verwerkersovereenkomst
Verwerkingsverantwoordelijke:
Verwerker:
Datum overeenkomst:
Datum beoordeling:

Privacycriterium
Een organisatie is verplicht om afspraken te maken (vaak in de vorm van verwerkersovereenkomsten) met partijen die ten opzichte van de organisatie (de verwerkingsverantwoordelijke) als verwerker zijn te kwalificeren. Daarbij gaat het om persoonsgegevens, afkomstig van de betrokkenen van de verwerkingsverantwoordelijke, die in het kader van het (sub)verwerkerschap worden verwerkt.
Norm(en): Art. 28 AVG

Privacyrisico('s)
Als organisaties ervoor kiezen om gebruik te maken van (sub)verwerkers, dan vereist de AVG dat met deze (sub)verwerkers afspraken worden vastgelegd. Dit gebeurt meestal in de vorm van een verwerkersovereenkomst. Deze overeenkomst moet ervoor zorgen dat de privacy en persoonsgegevens van betrokkenen op afdoende wijze worden beschermd. Als de organisatie niet afdoende haar (sub)verwerkers in kaart brengt en met hen overeenkomsten sluiten, loopt zij het risico op ongeoorloofd (her)gebruik, datalekken etc. Dit kan resulteren in reputatieschade en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.

Toetsingskader
Voorvragen: ☐ Is er een AVG Self-assessment door de verwerker ingevuld, en bevat deze voldoende informatie? ☐ Is de relatie tussen de ketenpartijen voldoende duidelijk? Bijv. door het bestuderen van de hoofdovereenkomst. ☐ Wordt er gebruik gemaakt van een standaard modelverwerkersovereenkomst van het Privacy Convenant?
Formele vereisten ☐ Onderwerp van de verwerkersovereenkomst ☐ Duur van de verwerking/overeenkomst ☐ Categorieën persoonsgegevens ☐ Aard en het doel van de verwerking ☐ Specifieke taken en verantwoordelijkheden van de verwerker

- ☒ Concrete risico's voor de rechten en vrijheden van de betrokkene
- ☐ Rechten en verplichtingen van de verantwoordelijke en verwerker
- ☐ Medewerkers van verwerker zijn verplicht tot geheimhouding van de persoonsgegevens die met verwerker worden gedeeld
- ☐ Instructie dat de verwerker de persoonsgegevens passend moet beveiligen
- ☐ Instructie dat de verwerker alleen persoonsgegevens verwerkt conform de instructie van de verantwoordelijke
- ☐ Instructie dat de verwerker alleen na uitdrukkelijke opdracht en instructie van de verantwoordelijke subverwerkers zal inschakelen
- ☐ Instructie dat contractuele bepalingen onverkort gelden voor door de verwerker ingeschakelde subverwerkers (ketenbeding)
- ☐ Verplichting dat de verwerker medewerking moet verlenen indien een betrokkene zijn rechten wenst uit te oefenen
- ☐ Verplichting dat na afloop van de overeenkomst met verwerker de persoonsgegevens worden teruggegeven of vernietigd (behoudens een op verwerker rustende wettelijke bewaarplicht)
- ☐ Verplichting dat verwerker medewerking verlenen aan door de verantwoordelijke uit te voeren inspecties en audits.
- ☐ Aansprakelijkheidsclausule
- ☐ Rechten en plichten voor de verwerker en de verantwoordelijke rondom de melding, medewerking en afhandeling van datalekken en beveiligingsincidenten

Red flags en plausibiliteitschecks:

- Realiteit kwalificatie verwerker/verwerkingsverantwoordelijke
- Risicovolle verwerkers (schoolfotograaf, kleinere verwerkers, educatieve apps, etc.)
- Verwerkersovereenkomst volgens het 'Privacyconvenant'
- Afspraken, het doel, de aard en de context van een verwerking zijn SMART
- Contractmanagement (koppeling verwerkersovereenkomst met bovenliggende overeenkomst)
- Verwerkingen buiten EU/EER
- Beperking verwerking tot legitieme doelen
- Verbod op het gebruik van de gegevens voor profiling, data analytics, marktonderzoek of advertenties
- Afspraken over hoe gegevens daadwerkelijk worden geanonimiseerd
- Afspraken over vernietiging of teruggave van persoonsgegevens na einde van (verwerkers)overeenkomst
- Daadwerkelijk beschrijving van genomen technische en organisatorische maatregelen (incl. herzieningsprotocol)
- Datalekken en beveiligingsincidenten vallen onder Security Protocol van verwerker
- Datalekken worden onmiddellijk, in alle redelijkheid en zonder onredelijke vorm van vertraging, aan de verantwoordelijke gemeld
- Verwerker handelt inzageverzoeken (mede) kosteloos af
- Overeenkomst voldoet aan aanvullende wet- en regelgeving (BW, Fw, WPG, Wet ED en Tw)
- Toepasselijkheid specifieke informatiebeveiligingsnormen (bijv. ISO 27000)

Analyse en opmerking(en):