Door beide Partijen in te vullen bijlagen bij de Model Verwerkersovereenkomst 4.0

Bijlage 1: Privacybijsluiter Cloudwise CAAS

Deze bijlage is onlosmakend verbonden met de Model Verwerkersovereenkomst 4.0 van Cloudwise zoals terug te vinden op www.cloudwise.nl/voorwaarden. De gebruikte definities verwijzen naar dit document waar ze nader worden toegelicht.

Deze bijlage heeft betrekking op het product **Cloudwise CAAS,** bedoelt voor cybersecurity-dienstverlening.

Deze bijlage heeft betrekking op de diensten binnen de Sophos MDR dienstverlening**.**

a) Contactgegevens

Voor vragen of opmerkingen over deze Privacybijsluiter of de werking van de genoemde producten kunt u terecht bij **Cloudwise**. Te bereiken via telefoonnummer 074 240 46 06.

b) Versienummer en versiedatum

Deze bijlage betreft **versie 2026.06**, gepubliceerd op **10-06-2026**.

c) Algemene informatie

Naam product en/of dienst	**Cloudwise CAAS**
Naam Verwerker en vestigingsgegevens	**Cloudwise te Hengelo**
Link naar Leverancier	https://www.cloudwise.nl
Link naar productpagina	https://cloudwise.nl/oplossingen/cybersecurity-as-a-service-caas
Beknopte uitleg en werking product en/of dienst	Cloudwise Cybersecurity As A Service (CAAS) is een combinatie van producten en diensten ten behoeve van cybersecurity-dienstverlening, bestaande uit diverse producten en diensten.
Doelgroep	PO, SO, VO en VSO.
Gebruikers	Medewerkers, leerlingen van eerdergenoemde doelgroep die zich binnen de cloudomgeving van Onderwijsinstelling bevinden.

d) Omschrijving specifieke producten en/of diensten

Cloudwise maakt onderscheid tussen verwerkingen die onlosmakelijk onderdeel vormen van de aangeboden dienst en (eventueel gebruikte) optionele verwerkingen.

1. *Verwerkingen die **onlosmakend onderdeel** vormen binnen Cloudwise CAAS:*

Omschrijving product en/of dienst	Bijbehorende verwerkingen
Sophos Managed Detection and Respone (MDR)	Sophos MDR combineert machine learning-technologie, AI en deskundige analyses voor verbeterde detectie van bedreigingen, diepgaander onderzoek van waarschuwingen en gericht acties om bedreigingen snel en nauwkeurig te elimineren.
Sophos XDR[1]	Sophos XDR is een endpoint product waarmee kritieke informatie van endpoints, servers, firewalls, email en andere producten wordt opgeslagen, toegankelijk is en kan worden gebruikt voor bedreigingsdetectie en -response. Apparaat- en loggegevens worden met regelmatige tussenpozen uit de producten opgehaald en opgeslagen in het Sophos Data Lake. Dit kan zowel een sensor als een volledigeagent zijn.

2. *Aanvullende **optionele producten en/of diensten** en bijbehorende Verwerkingen*

De volgende producten en diensten zijn optioneel in- of uit te schakelen door de Onderwijsinstelling. Deze maken allen, in meer of mindere mate, gebruik van de in dit document benoemde verwerkingen (dezelfde Persoonsgegevens). Per dienst is kort de werking toegelicht.

Omschrijving product en/of dienst	Bijbehorende verwerkingen
Sophos Managed Risk	Een oplossing voor het beheer van kwetsbaarheden, risicobeoordeling en externe aanvalsoppervlakten, gebaseerd op toonaangevende Tenable-technologie en geleverd als een beheerde service door Sophos. Deze service helpt bij het identificeren van blootstellingen die specifiek zijn voor de omgeving van de klant en biedt herstelmaatregelen om aanvallen te voorkomen.
Sophos Cloud Optix	Een AI-gestuurd beveiligings- en complianceplatform voor cloudomgegvingen. Biedt een realtime inventarisatie van cloudinfrastructuur, inclusief servers, opslag en netwerkelementen en helpt de beveiliging te bewaken en te voldoen aan compliancenormaen in één gebruikersinterface.
Firewall integratie	De Sophos Firewall Integration stelt de MDR-dienst in staat om netwerkverkeer te analyseren en te correleren met andere beveiligingssignalen. Hierdoor kunnen verdachte activiteiten sneller worden gedetecteerd en geclassificeerd. De firewall levert aanvullende context aan het Security Operations Center (SOC), wat bijdraagt aan een efficiëntere incidentrespons. Er worden geen persoonsgegevens opgeslagen in de firewall zelf; analyse vindt plaats op metadata en gedragskenmerken.

[1] Sophos XDR is de gebruikte software tbv de dienst Sophos MDR. Deze zijn onlosmakend aan elkaar verbonden.

Sophos NDR	Sophos NDR is een netwerkgebaseerde detectie- en responsoplossing waarmee kritieke informatie uit het interne netwerkverkeer wordt verzameld, opgeslagen en geanalyseerd voor dreigingsdetectie en -response. Netwerkstromen, metadata en afwijkende communicatiepatronen worden continu uit het netwerk gehaald en opgeslagen in het Sophos Data Lake. Hierdoor kunnen aanvallen worden herkend die buiten de endpoint-agent plaatsvinden, zoals laterale beweging, C2-verkeer of ongebruikelijke datastromen, ook op apparaten zonder agent (bijv. BYOD) dankzij sensoren op strategische posities in het netwerk.

e) Doeleinden voor het verwerken van persoonsgegevens[2]

In de volgende tabel staat weergegeven welke specifieke doeleinden van toepassing zijn op het product of de dienst.

Doeleinde	FORA-hoofdbedrijfsfunctie
De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens	ICT-ondersteuning (ICT Beheer)
De continuïteit, verbetering, goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning	ICT-ondersteuning (ICT Beheer)

f) Categoriën Persoonsgegevens inclusief bewaartermijnen

Bij het gebruik de MDR dienst worden de volgende persoonsgegevens verwerkt.

Onderstaande verwerkingen zijn van toepassing op alle gebruikersaccounts binnen de IT Omgeving die worden opgenomen in de CAAS dienstverlening. Dit betreft **Onderwijsdeelnemer (student/leerling)** en/of **Medewerker onderwijsinstelling**.

Verwerkingen

- **Contactgegevens** E-mailadres (school), (Voorna(a)m(en), voorletter(s), achternaam, aanschrijftitel zoals geslacht, E-mailadres (school));[3]

[2] Voor Onderwijsinstellingen is in de toelichting een overzicht opgenomen van de relatie tussen de in onderdeel E benoemde verwerkingsdoeleinden en de (hoofd)bedrijfsfuncties in de FORA. Onderwijsinstellingen kunnen aan de hand van dit overzicht in de toelichting de specifieke verwerkingsdoeleinden selecteren die van toepassing zijn, aangevuld met de (hoofd)bedrijfsfuncties in de FORA.

[3] Binnen de dienstverlening van Sophos wordt enkel het e-mailadres verwerkt. Overige contactgegevens zijn optioneel en enkel tbv van vastlegging van meldingen binnen het servicedesk-systeem van Cloudwise.

- **Gebruikersgegevens:**
  Gebruikersnaam, IP adressen, MAC adressen, Processes (waar commandos worden vastgelegd, dit kan gebruikersnamen, wachtwoord, API keys en credentials bevatten, Applicaties, Portable Executable (PE) bestanden, Browser add-ons en data van Microsoft Edge en Google Chrome (bijv. favorieten, cookies en browsergeschiedenis), gebruikersfolder (bijv. muziek, documenten, downloads, videos, afbeeldingen, bureaublad), Browser Addons, File Hashes, Hostnames, Poorten, System Events en Logs, URLs, crash- en memory dumps, Export van Windows Registry, third party application logs (bijv. OneDrive, DropBox, AV Software, password managers), Email adresses, Email subject data, Infrastructuur metadata (bijv. instances, VM's, storage buckets en securitygroepen), Network flows (bijv. welk IP adres communiceert met welk ip adres).

Bewaartermijn van de Persoonsgegevens of de criteria om die vast te stellen
90 dagen voor alle verzamelde data. Indien data is betrokken bij het incident, zal deze data daar vastgelegd worden. Gelogde incidenten worden tot 1 jaar bewaard (optioneel uit te breiden).

g) Locatie van opslag en Verwerking Persoonsgegevens

Opslag van alle data binnen Cloudwise CAAS vindt plaats binnen de EER:

	Verwerking	Land/Regio van opslag en verwerking
a)	Sophos MDR combineert machine learning-technologie, AI en deskundige analyses voor verbterde detectie van bedreigingen, diepgaander onderzoek van waarschuwingen en gericht acties om bedreigingen snel en nauwkeurig te elimineren.	EER
b)	Sophos XDR is een oplossing waarmee kritieke informatie van endpoints, servers, firewalls, email en andere producten wordt opgeslagen, toegankelijk is en kan worden gebruikt voor bedreigingsdetectie en -response. Apparaat- en loggegevens worden met regelmatige tussenpozen uit de producten opgehaald en opgeslagen in het Sophos Data Lake.	EER
c)	Een oplossing voor het beheer van kwetsbaarheden en externe aanvalsoppervlakten, gebaseerd op toonaangevende Tenable-technologien en geleverd als een beheerde service door Sophos. Deze service helpt bij het identificeren van blootstellingen die specifiek zijn voor de omgeving van de klant en biedt herstelmaatregelen om aanvallen te voorkomen.	EER
d)	Een AI-gestuurd beveiligings- en complianceplatform voor cloudomgegvingen. Biedt een realtime inventarisatie van cloudinfrastructuur, inclusief servers, opslag en netwerkelementen en helpt de beveiliging te bewaken en te voldoen aan compliancenormaen in één gebruikersinterface.	EER
e)	ServiceNow is de door Cloudwise gebruikte ITSM tool, bedoelt voor het registreren en verwerken van servicedesk-aangelegenheden (zoals bijvoorbeeld het vastleggen van cases). Hierin wordt contactinformatie opgeslagen.	EER

h) Subverwerkers

Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Ten tijde van het afsluiten van de Verwerkersovereenkomst, gebruikt Cloudwise de volgende Subverwerkers:

Naam	Omschrijving	Land/Regio van opslag en verwerking	Vestigingsland subverwerker
Sophos	Zie verwerkingen a t/m d	EER	Verenigd Koninkrijk
ServiceNow	Zie verwerking e	EER	Verenigde Staten

Paraaf

Onderwijsinstelling Cloudwise

Bijlage 1 (Privacybijsluiter) maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad, de verschillende betrokken ketenpartijen (MEVW, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u op www.privacyconvenant.nl.

Bijlage 2: Beveiligingsbijlage Cloudwise CAAS

Deze Beveiligingsbijlage is onlosmakelijk verbonden met de Verwerkersovereenkomst 4.0.
Dit betreft versienummer 2025.11, gepubliceerd op 01-11-2025.

Cloudwise heeft, overeenkomstig de AVG en artikel 7 en 8 van de Model Verwerkersovereenkomst passende technische en organisatorische maatregelen genomen om de verwerking van persoonsgegevens aantoonbaar te beveiligen. Deze bijlage geeft een beknopte beschrijving en opsomming van de maatregelen.

1) Maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking.

- Cloudwise heeft een passend beleid voor de beveiliging van de Verwerking van Persoonsgegevens
- Verwerker neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.
- Cloudwise heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van Persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Cloudwise heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.
- Cloudwise sluit met medewerkers geheimhoudingsverklaringen af en maakt informatiebeveiligingsafspraken.
- Cloudwise stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.

a) Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en applicatie te waarborgen

Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden. Cloudwise gebruikt hiervoor in beginsel het “Certificeringsschema informatiebeveiliging en privacy ROSA” (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide passend niveau van informatiebeveiliging en privacy.

Rapportage BIV-Classificatie			
Toetsvorm	Self-Assesment, uitgevoerd op 2-4-2026		
Uitvoerder toets	Jeroen Renard (Security Officer)		
BIV-Classificatie	Beschikbaarheid = Hoog, Integriteit = Hoog, Vertrouwelijkheid = Hoog		
Categorie	**Maatregel**	**Compliance**	**Uitleg**
Beschikbaarheid	Ontwerp	Voldaan	
	Capaciteit Beheer	Voldaan	
	Onderhoud	Voldaan	
	Testen	Voldaan	
	Monitoring	Voldaan	
	Herstel	Voldaan	
Integriteit	Herleidbaarheid (gebruikers)	Voldaan	
	Backup	Voldaan	
	Applicatie Controles	Voldaan	
	Onweerlegbaarheid	Voldaan	
	Herleidbaarheid (technisch beheer)	Voldaan	
	Controle integriteit	Voldaan	
	Onweerlegbaarheid (applicatie)	Voldaan	
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	
	Logische toegang	Voldaan	
	Fysieke toegang	Voldaan	
	Netwerk toegang	Voldaan	
	Scheiding omgevingen	Voldaan	
	Transport en fysieke opslag	N.v.t	
	Logging	Voldaan	
	Omgaan met kwetsbaarheden	Voldaan	

b) Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Verwerker heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zal Verwerker de Verwerkingsverantwoordelijke de volgende informatie ter hand stellen:

- de kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk; samenvatting van de inbreuk, waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op welk onderdeel van de beveiliging heeft het betrekking, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van Persoonsgegevens);
- de oorzaak van de inbreuk;
- hoe de inbreuk is ontdekt;
- de maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;
- of de bij de inbreuk betrokken Persoonsgegevens versleuteld, gehasht etc. waren;
- de groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep(en) Betrokkenen;
- wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de groep(en) Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor de groep(en) Betrokkene(n);
- de hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere Persoonsgegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

In geval van een (vermoeden van een) beveiligingsincident en/of Datalek, kunnen Onderwijsinstelling en Cloudwise in beginsel contact met elkaar opnemen via onderstaande contactgegevens, op volgorde van niveau.

Niveau	Functie	Contactmogelijkheid
0	Medewerker SOC / MDR team	Via telefoonnummer (volgt na onboarding)
1	Teamleider Engineering Sophos	Via telefoonnummer (volgt na onboarding)
3	Manager Operations Cloudwise	Via centrale receptie 074 240 46 06
4	Algemeen Directeur Cloudwise	Via centrale receptie 074 240 46 06

Paraaf

Onderwijsinstelling

Cloudwise

Bijlage 2 (Beveiligingsbijlage) maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad, de verschillende betrokken ketenpartijen (MEVW, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u op www.privacyconvenant.nl.