

# Privacy en security



De kwaliteit van de informatievoorziening wordt voornamelijk gedefinieerd in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Om de gegevens en informatiesystemen waarover we beschikken, op deze gebieden te kunnen beschermen is het noodzakelijk een informatiebeveiligings-beleid te hebben. ThiemeMeulenhoff waarborgt de informatiebeveiliging door uitvoering van haar informatiebeveiligingsbeleid.

ThiemeMeulenhoff is sinds 23 december 2017 ISO 27001:2013 gecertificeerd. Met deze belangrijke certificering voor het gebruiken en implementeren van een Information Security Management System (ISMS) kan ThiemeMeulenhoff haar klanten optimale beveiliging van haar informatie garanderen.

## Verwerkersovereenkomst

ThiemeMeulenhoff treedt op als verwerker van onderwijsinstellingen in het primair onderwijs, voortgezet onderwijs en het beroepsonderwijs conform het Convenant Digitale Onderwijsmiddelen en Privacy – Leermiddelen en toetsen. [www.privacyconvenant.nl](http://www.privacyconvenant.nl)

In de Verwerkersovereenkomst van ThiemeMeulenhoff wordt tussen onderwijsinstellingen en ons vastgelegd welke opdracht wordt gegeven tot verwerking van persoonsgegevens bij het gebruik van digitale leermiddelen. ThiemeMeulenhoff hanteert daarbij de 'Model Verwerkersovereenkomst', die onderdeel uitmaakt van het 'Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen'. De Verwerkersovereenkomst vormt onderdeel van onze licentievoorwaarden die op het gebruik van digitale leermiddelen van toepassing zijn. Deze Verwerkersovereenkomst kan worden gedownload voor de eigen administratie. Als een onderwijsinstelling een getekend exemplaar wil ontvangen kan het ingevulde format gestuurd worden naar [privacy@thiememeulenhoff.nl](mailto:privacy@thiememeulenhoff.nl).

## Privacy bijsluiter

In de privacy bijsluiter van ThiemeMeulenhoff richten we ons tot de onderwijsinstelling met meer specifieke informatie over onze digitale leermiddelen en de bijbehorende gegevensverwerkingen. Zo wordt duidelijk welke opdracht de onderwijsinstelling ThiemeMeulenhoff geeft voor gegevensverwerking. De privacy bijsluiter helpt tevens bij het informeren van ouders en leerlingen over de verwerking van persoonsgegevens. De bijsluiter wordt jaarlijks geactualiseerd en is te vinden op: [www.thiememeulenhoff.nl/privacy](http://www.thiememeulenhoff.nl/privacy).

## Beveiligingsmaatregelen Edustandaard

Partijen zorgen er voor dat de beveiligingsmaatregelen worden genomen die zijn vastgesteld door Edustandaard en Edu-K conform het certificeringsschema informatiebeveiliging en privacy ROSA (zoals gepubliceerd op [https://www.edustandaard.nl/standaard\\_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/](https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/)).

## Veilige Email

Diverse processen maken gebruik van emailverkeer. Het bewustzijn op het gebied van informatiebeveiliging neemt gestaag toe en dit geldt ook voor de veiligheidsstandaarden voor e-mail. De belangrijkste doelstelling is om (verzendende) gebruikers zich te laten realiseren, dat het gaat om het zorgvuldig omgaan met gegevens van de eigen organisatie, van leerlingen en docenten, waarbij veilig mailen puur een middel is. Daarnaast kunnen ontvangende partijen bij een goede 'technische' inrichting van mail, automatische besluiten nemen of informatie vanuit een betrouwbare bron is verzonden. Dit voorkomt op termijn steeds meer 'phishing', en het ontvangen van mail in een SPAM folder.

Het verdient aanbeveling, voor zover dat al niet gebeurt, om van de emailstandaarden SPF, DKIM en DMARC gebruik te gaan maken, om daarmee 'veilige email' binnen de onderwijssector te vergroten. ThiemeMeulenhoff heeft deze standaarden momenteel geïmplementeerd.

## Telefoongesprekken klantenservice

Alle telefoongesprekken met de klantenservice van ThiemeMeulenhoff worden primair met de volgende twee doeleinden opgenomen: voor trainings- en coachingsdoeleinden en voor de onweerlegbaarheid van een contract; als de consument/Onderwijsinstelling telefonisch iets koopt of een contract afsluit en de eventuele bijbehorende klachtafhandeling.

Bij alle telefoongesprekken wordt aan het begin van het gesprek door een geautomatiseerde voice-over aangegeven dat het gesprek wordt opgenomen. De opnames worden niet langer bewaard dan strikt noodzakelijk (maximaal 1 jaar) en zijn niet toegankelijk voor onbevoegden. Voicelogs vallen ook onder de inzage, correctie en verwijderingsprocedure van ThiemeMeulenhoff.

## Datalek en Incident Response Procedure

In het geval er beveiligingsrisico's worden geconstateerd kan contact op worden opgenomen met de klantenservice van ThiemeMeulenhoff, [www.thiememeulenhoff.nl/contact](http://www.thiememeulenhoff.nl/contact). Of er kan een e-mail worden gestuurd naar [privacy@thiememeulenhoff.nl](mailto:privacy@thiememeulenhoff.nl).

ThiemeMeulenhoff heeft een Incident en Response Procedure ingericht.

- *De wijze waarop monitoring en identificatie van Datalekken plaatsvindt*  
ThiemeMeulenhoff monitort haar dienstverlening en heeft maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren. Signalen die duiden op een Datalek worden beoordeeld door het ISMS proces, onder verantwoordelijkheid van de security, risk en compliance officer van ThiemeMeulenhoff, die analyseert of sprake kan zijn van een Datalek.
- *De wijze waarop informatie wordt gedeeld:*  
Wanneer zich een Datalek voordoet, wordt de verantwoordelijke onderwijsinstelling door of namens ThiemeMeulenhoff in beginsel binnen 72 uur na vaststelling dat sprake is van een Datalek per e-mail geïnformeerd. Afhankelijk van de situatie, kan ook informatie worden gedeeld via onze website en officiële sociale media kanalen en/of officiële distributeurs en/of handelsagenten. Voor vervolgacties of vragen kan telefonisch of per e-mail contact worden

opgenomen met onze helpdesk via de in de Privacy Bijsluiter opgenomen gegevens, of via een nader te bepalen instructie die centraal gecommuniceerd zal worden in het geval van een calamiteit.

- *ThiemeMeulenhoff deelt ten minste de volgende informatie wanneer zich een datalek voordoet:*
  - De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
  - De oorzaak van het beveiligingsincident;
  - De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
  - Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
  - De omvang van de groep betrokkenen;
  - Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

Indien een concrete situatie zich daartoe leent, in het geval van een generiek datalek, dan zal ThiemeMeulenhoff een (eerste) melding van een datalek doen aan de Autoriteit Persoonsgegevens. De Onderwijsinstelling wordt hierover geïnformeerd en blijft ook in dit geval eindverantwoordelijk voor de melding.

In de gevallen van een datalek waarin beide partijen betrokken zijn, of waarin ondersteuning kan worden geboden met aanvullende informatie, wordt maximaal ingezet om het datalek te herstellen, de gevolgen te minimaliseren en elkaar hierover te informeren.