

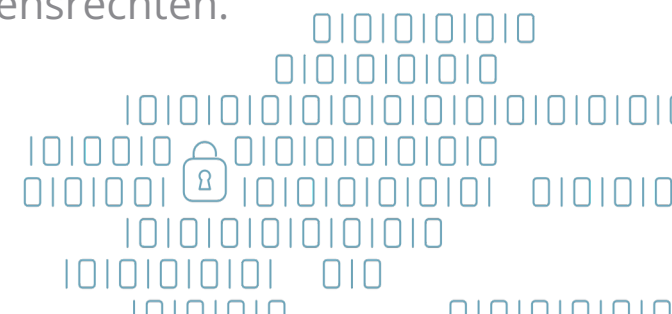
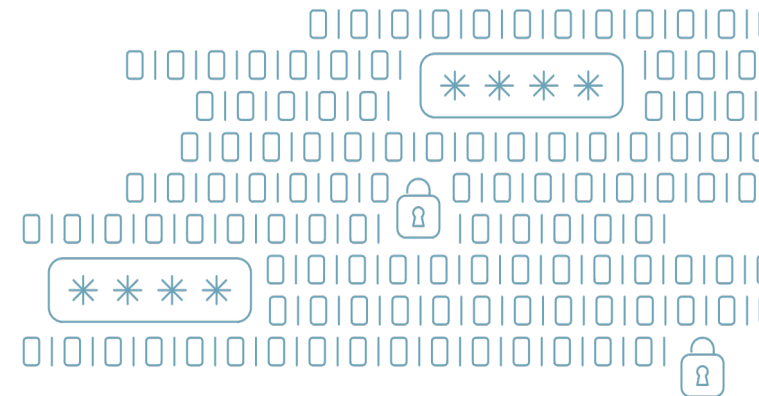
AVG en Moodle:

Privacy by design



Inhoudsopgave

- 1. Samenvatting
- 2. Waarom de privacy van gegevens belangrijk is
- 3. Privacy by design: hoe Moodle gegevensbescherming in zijn DNA integreert
- 4. Controle, keuze en naleving
- 5. Moodle versus de markt: privacy met de mens centraal
- 6. Hosting en verantwoordelijkheid: het belang van de juiste partner
- 7. Praktische privacy: wat elke Moodle-site zou moeten doen
- 8. Product in de schijnwerpers: privacy gerichte platforms voor ondernemingen, onderwijs en de publieke sector
- 9. Vooruitblik: een wereldwijd perspectief op leren en gegevensrechten.
- 10. Klaar om de volgende stap te zetten?



Samenvatting

Gegevensbescherming is niet langer slechts een wettelijke verplichting; het is een fundamentele verwachting van gebruikers en organisaties wereldwijd. Nu digitale platforms steeds kritischer worden geëvalueerd, onderscheidt Moodle Pty Ltd zich door een toewijding aan transparantie, controle en gebruikersbescherming die in elke laag van ons ecosysteem is geïntegreerd.

In deze whitepaper wordt onderzocht hoe Moodle Pty Ltd omgaat met gegevensbescherming binnen Moodle LMS, Moodle Workplace en de Moodle-app.

De rol van LTNC, als Moodle Certified Partners, is het bieden van betrouwbare, privacy gerichte leeromgevingen. In tegenstelling tot commerciële platforms die gebruikersdata te gelde maken of de controle beperken, stelt Moodle Pty Ltd organisaties in staat om hun data te beheren zoals zij dat wensen, ondersteund door een wereldwijde gemeenschap, privacy gerichte tools en flexibele hostingopties.

In deze whitepaper bespreken we:

- X** De privacyprincipes en ontwerpkeuzes achter Moodle.
- X** Hoe Moodle zich verhoudt tot commerciële platformen – en waar de valkuilen zitten.
- X** Praktische privacy maatregelen die elke instelling direct kan toepassen.
- X** Wat regelgeving zoals de AVG betekent voor een ethische leeromgeving.

Moodle LMS is meer dan een leermanagementsysteem; het is een alternatief dat de privacy respecteert in een wereld die deze te vaak negeert. Dit document fungeert zowel als een leidraad als een oproep tot actie: leertechnologen, instellingen en partners dienen gegevensbescherming centraal te stellen in hun praktijk en tools te selecteren die de mens centraal stellen.



Waarom de bescherming van gegevens belangrijk is

Van universiteiten en overheidsinstellingen tot internationale bedrijven: organisaties worden tegenwoordig geconfronteerd met steeds grotere hoeveelheden persoonsgegevens. Of het nu gaat om de voortgang van een student, de evaluatie van een medewerker of het certificaat van een burger, de verwachting is helder: gegevens moeten worden beschermd, verantwoord worden behandeld en nooit worden misbruikt.

Maar deze verwachting staat vaak haaks op de realiteit. Wereldwijd worden digitale platforms bekritiseerd vanwege ondoorzichtige datapraktijken, invasieve tracking en beperkte gebruikerscontrole. In sommige gevallen hebben hulpmiddelen die zijn ontworpen voor gemak of schaalbaarheid juist het vertrouwen ondermijnd waarop leeromgevingen zijn gebaseerd.



De privacykwesties in EdTech en werkplektools

De verschuiving naar digitaal leren – versneld door wereldwijde gebeurtenissen zoals de COVID-19-pandemie – heeft het bewustzijn van gegevensrechten vergroot.

Opmerkelijke onderzoeken naar leveranciers van EdTech hebben onthuld hoe sommige platforms gegevens verzamelen en verhandelen buiten hun educatieve of trainingsdoeleinden, vaak zonder expliciete toestemming. Voor trainingen op de werkplek, compliancetools en leerapps zijn de zorgen over tracking door derden en datagebruik voor uiteenlopende doeleinden evenzeer reëel.

Bij Moodle Pty Ltd hanteren we een alternatieve benadering: een benadering die is gebaseerd op **privacy by design** en wordt gedreven door onze missie, niet door winstbejag. Als gecertificeerde B Corporation met een wereldwijd bereik, richten we ons op het ontwikkelen van tools die ethische, door de gebruiker gecontroleerde leeromgevingen bevorderen.

Veiligheid door ontwerp

Moodle Pty Ltd hanteert een '[security en privacy by design](#)'-benadering voor ontwikkeling, afgestemd op wereldwijde standaarden zoals de [OWASP Top Ten](#) en [CIS Controls](#). We voeren een wereldwijd programma uit voor het [openbaar maken van kwetsbaarheden via Bugcrowd](#) en zorgen ervoor dat elke nieuwe functie vóór de release wordt geëvalueerd op potentiële risico's.

Voor een uitgebreid overzicht van de wijze waarop wij beveiliging integreren in ons platform, verwijzen wij naar het [whitepaper Moodle-beveiliging](#). Vertrouwen opbouwen door middel van open samenwerking.



Privacy is essentieel voor leren en vertrouwen

Privacybescherming gaat niet alleen over regelgeving, maar ook over vertrouwen. Studenten, medewerkers en burgers moeten erop kunnen vertrouwen dat hun gegevens veilig zijn en uitsluitend worden gebruikt voor het beoogde doel. Pas dan durven zij volledig te participeren en zich te ontwikkelen.

Gegevensprivacy is gebaseerd op:

- X Vertrouwen** in de leeromgeving
- X Naleving** van internationale regelgeving zoals [AVG](#), [FERPA](#), [POPIA](#) en [HIPAA](#)
- X Controle** voor organisaties om hun eigen systemen te beheren gegevensstromen

Of je nu geaccrediteerde diploma's verstrekt, nieuw personeel opleidt of grootschalige vaardigheidsprogramma's beheert, de integriteit van jouw platform en de beslissingen die het neemt met betrekking tot data zijn nog nooit zo cruciaal geweest.

Privacy by design: Hoe Moodle gegevensbescherming in zijn DNA integreert

Hoewel **privacy** en **beveiliging** vaak door elkaar worden gehaald, zijn het twee verschillende concepten die echter nauw met elkaar verbonden zijn. **Beveiliging** richt zich op het beschermen van gegevens tegen ongeautoriseerde toegang, inbreuken of misbruik. **Privacy** daarentegen betreft het waarborgen dat de gegevens van een individu op een begrijpelijke en instemmende wijze worden verzameld, gebruikt en gedeeld.

Een platform kan veilig zijn zonder de privacy te respecteren, maar niet andersom. Daarom hanteert Moodle Pty Ltd een holistische benadering: een robuuste beveiligings-architectuur combineren met een diep respect voor de privacy van gebruikers. Van Moodle LMS tot Moodle Workplace en de Moodle App: onze producten zijn ontworpen om organisaties controle te bieden, compliance te waarborgen en de rechten van elke gebruiker te beschermen.



Transparant en gebruikersgericht

Moodle is ontwikkeld om organisaties – en niet leveranciers – de controle te bieden over de opslag, het beheer en de toegang tot gegevens. Of de data nu on-premises wordt gehost of bij een Moodle Certified Partner, sitebeheerders hebben inzicht in:

- X Wie heeft toegang tot de gegevens?
- X Welke gegevens worden verzameld?
- X Waar worden de gegevens opgeslagen?
- X Hoe lang worden ze bewaard?

Hulpmiddelen voor het publiceren van beleid, het beheren van gebruikersinstellingen en het beoordelen van dataverzoeken zijn in het platform geïntegreerd, waardoor de naleving van lokale regelgeving zoals AVG, POPIA en FERPA wordt vereenvoudigd.

Ontworpen voor verschillende omgevingen

Moodle biedt een uitgebreid scala aan implementatiebehoeften – van veilige offline overheidsnetwerken tot openbare cloudnetwerken – en garandeert consistente privacybescherming in alle omgevingen. Rolgebaseerde toegang, encryptieprotocollen en toestemmingsfuncties op gebruikersniveau stellen overheden, universiteiten en bedrijven in staat hun installaties te personaliseren en tegelijkertijd te voldoen aan gangbare privacystandaarden.

Deze flexibiliteit stelt Moodle in staat om te opereren in complexe omgevingen met meerdere belanghebbenden, zonder dat dit ten koste gaat van de gegevensbescherming. Bovendien kunnen onze modulaire en open producten privacyfuncties uitbreiden, aanpassen of integreren met interne compliance-workflows.



Controle, keuze en naleving

Privacy van gegevens betreft niet alleen de wijze waarop een platform met jouw gegevens omgaat, maar ook wat het je toestaat te doen met die gegevens. Bij Moodle Pty Ltd zijn we van mening dat organisaties volledige controle moeten hebben over de verzameling, het beheer, de opslag en het wissen van gegevens. Onze rol is om de benodigde tools, flexibiliteit en transparantie te bieden ter ondersteuning van die controle, ongeacht waar of hoe een Moodle-platform wordt geïmplementeerd.



Volledig eigendom en autonomie

In tegenstelling tot veel andere platformen verplicht Moodle software je niet tot één specifieke werkwijze. Of je nu een bedrijfstrainingsprogramma, een nationaal onderwijsportaal of een universiteitsbrede virtuele leeromgeving beheert, jij blijft de gegevensbeheerder.

Moodle biedt je:

- X Keuzevrijheid** om te bepalen waar en hoe uw gegevens worden gehost
- X Fijnmazige controle** over toegang tot gegevens en gegevensbewaring
- X Hulpmiddelen voor het publiceren, volgen en handhaven van gegevensbeleid**
- X Ingebouwde ondersteuning** voor gebruikersconsent en wettelijke leeftijdsverificatie

Deze mate van autonomie is met name waardevol in gereguleerde omgevingen, waar naleving van wetgeving zoals AVG essentieel is en waar controle over gegevensstromen een kwestie van juridisch en organisatorisch risico vormt.

Ingebouwde nalevingstools

Moodle software biedt een scala aan functies waarmee organisaties hun privacy verplichtingen kunnen naleven en compliance kunnen aantonen:

- X** Beleidsbeheerder: Publiceer verplichte en optionele beleidsregels waaraan gebruikers moeten voldoen voordat zij toegang krijgen tot het platform.
- X** Leeftijdsverificatie: Toepassen van de minimumleeftijdseisen op basis van jouw rechtsgebied.
- X** Gegevensverzoeken: Hiermee kunnen gebruikers een kopie van hun gegevens aanvragen of verzoeken om deze te laten verwijderen.
- X** Gegevensregister: behoud een centraal overzicht van alle soorten persoonlijke gegevens die op jouw Moodle-site zijn opgeslagen, incl. doeleinden en de bewaartermijnen.
- X** Rol van de functionaris voor gegevensbescherming: Ken de verantwoordelijkheid toe voor het toezicht op het privacybeheer binnen jouw organisatie.

Deze hulpmiddelen zijn beschikbaar in Moodle LMS en Moodle Workplace. In Workplace zijn extra beheerdersrechten en multi-tenant-bedieningselementen beschikbaar voor het beheer van naleving binnen afdelingen, instanties of klantgroepen.



Naleving zonder concessies

Sommige platforms beweren compliance te ondersteunen, maar bieden weinig inzicht in waar gegevens worden opgeslagen of welke derden toegang hebben. Moodle Pty Ltd hanteert een tegenovergestelde benadering. Door jou de *keuze* te bieden uit infrastructuur, transparante documentatie en toegang tot het onderliggende systeem, ondersteunen wij je bij het implementeren van privacy procedures die aansluiten bij het beleid van jouw organisatie – niet alleen bij dat van ons.

Als Moodle Certified Partner biedt LTNC verbeterde compliance-diensten, waaronder audit-klaar hosting, regelmatige updates en gegevensverwerking volgens internationale normen zoals ISO 27001 en 9001.



Wij adviseren je om gerichte vragen te stellen om inzicht te verkrijgen in de wijze waarop jouw hosting-partner (of welke leverancier dan ook) omgaat met belangrijke privacy vraagstukken:



Hoe worden persoonlijke gegevens opgeslagen, beveiligd en geback-up't?



Welke certificeringen en audits bestaan er op het gebied van privacy en beveiliging?



Hoe worden software-updates en beveiligingspatches beheerd?



Waar worden de gegevens fysiek gehost en voldoet dit aan uw regionale eisen?

Als ISO 27001 gecertificeerde Moodle Partner beantwoorden wij deze vragen graag in een vrijblijvend gesprek.

Moodle versus de markt:

Privacy die de mens centraal stelt

In een tijdperk van data-exploitatie en ondoorzichtige platformpraktijken onderscheidt Moodle als product zich. Terwijl andere leerplatformen worden bekritiseerd om intrusieve dataverzameling, op surveillance gebaseerde bedrijfsmodellen of beperkte transparantie, kiezen wij voor een andere benadering – een benadering die is gebaseerd op respect, niet op winst.

Wij verkopen geen gebruikersgegevens. Wij plaatsen geen advertenties. Wij volgen gebruikers niet op het internet.

In plaats daarvan hechten wij waarde aan gebruikerscontrole, institutioneel eigenaarschap en langdurig vertrouwen.

Een toenemende vertrouwenskloof in digitaal leren

Recent onderzoek heeft aangetoond dat veel EdTech- en corporate learning-platforms aanzienlijk meer data verzamelen dan noodzakelijk, vaak zonder dat gebruikers zich hiervan volledig bewust zijn. Sommige platforms maken gebruik van gedragsregistratie, delen gegevens met adverteerders of bieden beperkte mogelijkheden om zich af te melden. Zelfs wanneer tools gratis of gesubsidieerd zijn, kunnen gebruikers mogelijk met hun data betalen.

Overheidsinstanties, universiteiten en bedrijven geven terecht tegengas: zij eisen platforms die de principes van toestemming, doelbinding en dataminimalisatie respecteren.



Onze privacy belofte

Moodle LMS bieden een geloofwaardig alternatief:

- X Open, inspecteerbare code:** iedereen kan verifiëren hoe gegevens worden verwerkt, zonder black boxes.
- X Gebruikersgericht ontwerp:** aspecten zoals beleid Beheer, hulpmiddelen voor gegevensaanvragen en op rollen gebaseerde autorisaties zijn geïntegreerd.
- X Ethische fundamenten:** Als doelgerichte organisatie en gecertificeerde B Corporation zijn onze prikkels gericht op het algemeen belang, niet op het rendement voor aandeelhouders.
- X Modulaire architectuur:** Je kiest zelf welke plug-ins, Integraties en gegevensspaden worden gebruikt (niet door ons).

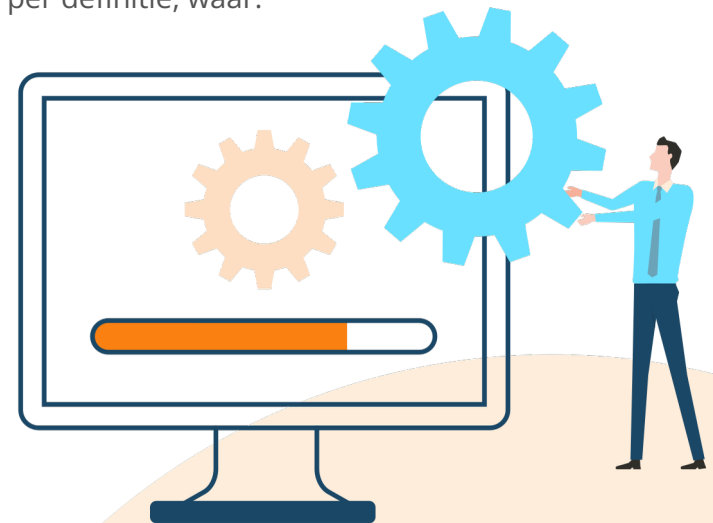
De privacygerichte benadering van Moodle LMS wordt vooral gewaardeerd door:

- X Overheidsinstellingen** die streven naar soevereine controle en afstemming op nationale data-strategieën.
- X Hogescholen en universiteiten** die onderworpen zijn aan wetgeving ter bescherming van studenten en normen voor academische integriteit.
- X Bedrijven en non-profitorganisaties** die werknemersgegevens en naleving in alle wereldregio's beheren.

Niet alleen compliant, maar ook transparant

In tegenstelling tot bepaalde aanbieders die compliance als een formaliteit beschouwen, is zijn wij van mening dat privacy begrijpelijk en uitlegbaar moet zijn. De Moodle LMS documentatie en ontwikkelingsproces is transparant. De functies binnen Moodle LMS zijn ontworpen om organisaties de helderheid te bieden die zij nodig hebben om te voldoen aan zowel wettelijke als ethische verplichtingen.

Waar anderen verhullen, onthult Moodle LMS. Waar anderen beperken, stelt Moodle LMS in staat. In een competitieve markt van platforms die privacybeloften doen, maakt Moodle LMS deze – per definitie, waar.



Hosting en verantwoordelijkheid: Waarom de juiste partner essentieel is

Een veilig platform dat de privacy respecteert, draait niet alleen om de software, maar ook om de wijze en locatie van hosting. Zelfs de best ontworpen tools kunnen kwetsbaar worden wanneer ze worden geïmplementeerd zonder de juiste controles, monitoring of governance. Bij Moodle Pty Ltd beschouwen we hosting niet enkel als een infrastructuurbeslissing, maar als een essentiële laag in de bescherming van privacy.



Controle over uw gegevens, vanaf de basis

Moodle biedt organisaties de mogelijkheid om een hostingomgeving te selecteren die aansluit bij hun privacyvereisten, risicobereidheid en interne capaciteiten.

Moodle LMS kun je zelf downloaden en hosten. Moodle Workplace is uitsluitend beschikbaar via de Moodle Certified Partner.

Ongeacht het model blijft één principe onveranderd: Jij blijft de eigenaar van jouw gegevens.

- X** Jij bepaalt waar gegevens worden opgeslagen en wie er toegang toe heeft.
- X** Jij configureert data-retentie binnen Moodle via de ingebouwde privacy-tools.
- X** Jij selecteert een hosting partner met een bewaarbeleid en back-up strategie die aansluit bij jouw eisen.

De functie van Moodle Certified Partners

Voor organisaties met aanzienlijke nalevingsverplichtingen, zoals overheidsinstellingen, multinationals of universiteiten die vertrouwelijke gegevens van studenten verwerken, kan samenwerking met een Moodle Certified Partner zorgen voor jouw gemoedsrust en verhoogde verantwoording bieden.

Gecertificeerde partners bieden hostingomgevingen die specifiek zijn geoptimaliseerd voor Moodle. Om te waarborgen dat jouw provider voldoet aan je privacy- en compliancebehoeften, kun je verifiëren of zij het volgende aanbieden:

- X AVG-conforme gegevensverwerking
- X Regelmatige software- en beveiligingsupdates
- X Encryptie in rust en tijdens transport
- X Auditklare logging- en back-upsystemen
- X Ondersteuning voor complexe implementaties of multi-enancy-structuren

Met deze vragen kunt je evalueren of jouw hosting-partner in staat is om veilig en privacygericht leren op grote schaal te ondersteunen.

Gecertificeerde partners kunnen je ook ondersteunen bij leveranciersrisicobeoordelingen, regionale vereisten voor gegevensresidentie en interne privacyaudits. Hierdoor zijn zij een strategische keuze voor duurzame naleving op de lange termijn.

De risico's van ondoorzichtige of onbeheerde hosting.

Platforms die de toegang tot back-endinstellingen beperken, geen inzicht bieden in datastromen of kritieke patches vertragen, vormen daarentegen een aanzienlijk risico. Slecht beheerde omgevingen kunnen leiden tot:

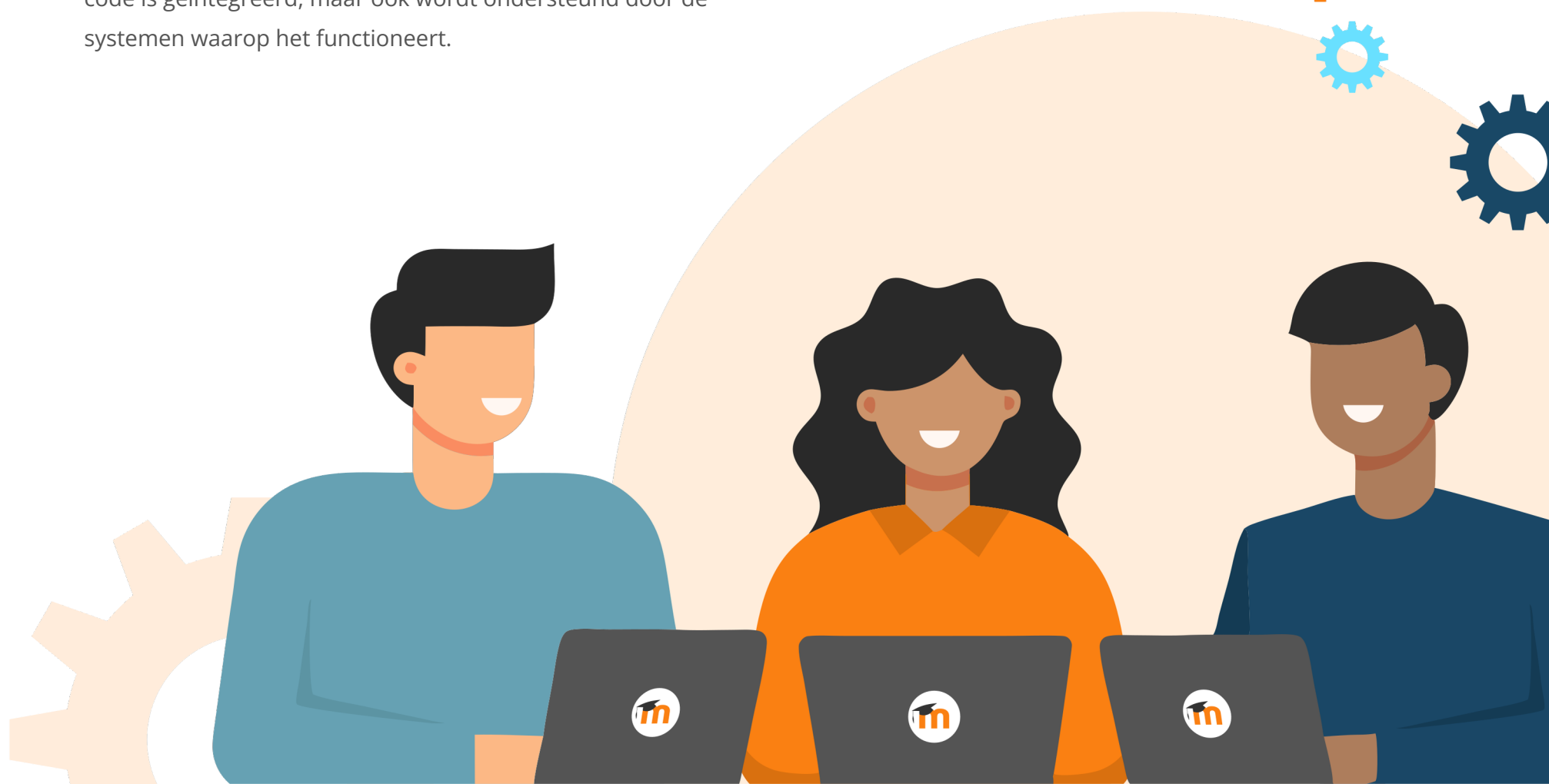
- X Datalekken door niet-gepatchte software
- X Onbedoelde blootstelling door onjuist geconfigureerde machtigingen
- X Onvermogen om te voldoen aan verzoeken om toegang, export of verwijdering
- X Regelgevende sancties bij niet-naleving

Privacy is niet slechts een functie; het is een gewoonte. Deze gewoonte moet zich uitstrekken tot de infrastructuur waarop jouw platform steunt.



Privacy als gezamenlijke verantwoordelijkheid

Bij Moodle beschouwen we dataprivacy als een gezamenlijke verantwoordelijkheid: tussen ons als platformprovider, jou als site-eigenaar en – indien van toepassing – jouw hostingpartner. Door open architectuur te combineren met betrouwbare serviceproviders, waarborgt Moodle dat privacy niet alleen in de code is geïntegreerd, maar ook wordt ondersteund door de systemen waarop het functioneert.



Praktische privacy: Wat elke Moodle-site zou moeten doen

Hoewel Moodle de tools, functies en architectuur biedt ter ondersteuning van gegevensprivacy, ligt de uiteindelijke naleving bij de organisatie die het platform gebruikt. Of je nu een trainingsportaal voor de overheid, een inwerkprogramma voor bedrijven of een omvangrijk universitair LMS beheert, proactief privacybeheer is van cruciaal belang.

In dit gedeelte worden de aanbevolen praktijken voor Moodle-sitebeheerders uiteengezet om de bescherming van de privacy te verbeteren en te voldoen aan lokale wettelijke vereisten.

1.

Publiceer en beheer het privacybeleid van uw website

Gebruik de beleidshandler van Moodle om overeenkomsten voor beleidsregels te creëren, weer te geven en te beheren, zoals:

- X Privacyverklaring van de website
- X Openbaarmaking van cookies of analyses
- X Voorwaarden voor dienstverlening of acceptabel gebruik
- X Leeftijd/duur van toestemming (indien van toepassing)

Beleid kan verplicht of optioneel zijn en kan worden gekoppeld aan specifieke gebruikersrollen of -activiteiten.



2.

Wijs een functionaris voor gegevensbescherming aan

Wijs een medewerker of team aan dat verantwoordelijk is voor het beheer van de gegevensbescherming op jouw site. Moodle biedt een functie als privacyfunctionaris met specifieke bevoegdheden om:

- X Bekijk en beheer verzoeken om gebruikersgegevens.
- X Beoordelen van verwijderen en exporteren van gegevens.
- X Houd toezicht op de bewaartermijnen in het gegevensregister.

Hiermee wordt gegarandeerd dat er heldere verantwoording en toezicht is voor alle privacygerelateerde handelingen.



3.

Gebruikersgegevensverzoeken activeren en beantwoorden

Moodle faciliteert de volledige levenscyclus van verzoeken om inzage en verwijdering van gegevens, waaronder:

- X Verzoek om het downloaden van persoonlijke gegevens.
- X Verzoek om gegevensverwijdering (o.v.v. bewaartermijnen).
- X De status van het verzoek bekijken in het gebruikersprofiel.

Met deze functies kunt je voldoen aan de verplichtingen die voortvloeien uit wetgeving zoals de AVG, FERPA of andere regionale kaders voor gegevensbescherming.

4. Gebruik het gegevensregister om bewaarbeleidsregels te definiëren

Met het gegevensregister kunt je het volgende vastleggen:

- X Welke soorten persoonsgegevens worden opgeslagen?
- X Waarom wordt elk gegevenstype verzameld?
- X De wettelijke basis voor de verwerking.
- X Bewaartermijnen en mogelijkheden voor automatische verwijdering.

Dit register biedt een duidelijk overzicht van de interne governance en externe audits.

5. Zorg indien nodig voor leeftijdsgebonden toegang

Als jouw site zich richt op jonge leerlingen, kan Moodle barrières voor digitale leeftijdsgrenzen handhaven en indien nodig toestemming van ouders vastleggen. Op deze manier kunt je voldoen aan regelgeving zoals AVG.

6. Gebruik rollen en machtigingen om de toegang tot gegevens te reguleren

Beperk de toegang tot persoonsgegevens door gebruik te maken van het gedetailleerde rollen- en machtigingssysteem van Moodle. Opleidingsbegeleiders in een zakelijke context zouden enkel toegang moeten hebben tot de voortgang van hun directe team, en niet tot gegevens binnen de gehele organisatie.

7. Controleer de beveiligingsinstellingen van uw website

Sterke privacy is afhankelijk van robuuste beveiliging. Controleer regelmatig het beveiligingsoverzicht en zorg ervoor dat:

- X HTTPS wordt op alle pagina's verplicht gesteld.
- X Standaardrollen beschikken over de noodzakelijke machtigingen.
- X Sessieverwerking en wachtwoordbeleid zijn actueel.



8. Werk samen met deskundigen indien je ondersteuning nodig hebt

Voor organisaties met beperkte interne middelen kan een samenwerking met een Moodle Certified Partner garanderen dat best practices worden geïmplementeerd en in de loop der tijd worden onderhouden.

Deze checklist is niet uitputtend, maar vormt een waardevol startpunt. Zelfs de implementatie van enkele van deze praktijken kan de risico's aanzienlijk verminderen, het vertrouwen van gebruikers vergroten en de naleving optimaliseren.



9. Versleutelde pushmeldingen activeren in de Moodle-app

Schakel bij het gebruik van de Moodle-app ondersteuning in voor end-to-end versleutelde pushmeldingen om gebruikersberichten tijdens de overdracht te beschermen. Deze optionele functie voegt een extra laag van privacy toe en garandeert dat gevoelige informatie, zoals opdrachtherinneringen of cijfermeldingen, veilig wordt verzonden, zelfs via mobiele netwerken. Lees meer over de beveiliging van de Moodle-app.

Product in de schijnwerpers: Privacygerichte platforms voor bedrijven, onderwijs en de publieke sector

Hoewel de kernfilosofie van Moodle met betrekking tot privacy voor alle producten geldt, biedt elk platform specifieke functies en configuraties die zijn afgestemd op diverse gebruikssituaties. Hier lees je hoe gegevensprivacy wordt benaderd in Moodle Workplace en de Moodle-app.

Moodle Workplace: privacy op grote schaal

Moodle Workplace breidt Moodle LMS uit met zakelijke functionaliteiten, waaronder multi-tenancy, geavanceerde rapportage en automatisering. Het is ontwikkeld voor organisaties die gestructureerde training op grote schaal aanbieden, zowel intern als extern.

Moodle Workplace maakt gebruik van een gedeelde databasestructuur, waarbij de privacygrenzen tussen huurders strikt worden gehandhaafd. Standaard worden er geen persoonsgegevens gedeeld tussen huurders. Gebruikers zijn zich niet bewust van het bestaan van andere huurders. Dit waarborgt een AVG-conforme gegevensscheiding in het ontwerp. Beheerders hebben de mogelijkheid om zichtbaarheidsinstellingen te configureren voor specifieke gebruikssituaties, maar het delen tussen huurders moet expliciet worden ingeschakeld.

Belangrijke privacykenmerken zijn:

- X Gegevenssegmentatie en rolbereik:** elke huurder opereert als een autonome gegevensomgeving, met unieke configuraties voor machtigingen, rollen en rapportages.
- X Aanpasbare richtlijnen voor gegevensbewaring en toestemming:** Definieer de bewaartermijn van gegevens en de wijze waarop toestemming wordt verkregen, per huurder of doelgroep.
- X Ondersteuning voor gedecentraliseerde toegangscontrole:** Wijs lokale beheerders toe binnen huurders en behoud wereldwijd toezicht.
- X Ontworpen voor gereguleerde en uiterst conforme omgevingen** binnen de overheid en het bedrijfsleven, de publieke sectoren.

Waar bepaalde rechtsgebieden of institutioneel beleid fysieke scheiding van gegevens tussen entiteiten vereisen, adviseert Moodle om afzonderlijke Moodle-instanties te implementeren in plaats van uitsluitend te vertrouwen op logische scheiding. Deze flexibiliteit waarborgt naleving zonder in te boeten op privacy of prestaties.

In samenwerking met een Moodle (Premium) Certified Partner biedt Moodle Workplace een robuuste basis voor schaalbare, auditklare leersystemen met geïntegreerde privacybescherming.



Moodle-app: mobiele privacy in het ontwerp

De Moodle-app biedt de leerervaring op mobiele apparaten, zonder in te boeten op privacy.

- X Geen tracking of gegevensverzameling door de Moodle-app** wanneer je verbinding maakt met jouw site.
- X Alle communicatie vindt rechtstreeks plaats** tussen de gebruiker en de site, niet via derden.
- X Optionele gecodeerde pushmeldingen**, beheerd door de instelling: Wanneer deze functie is ingeschakeld, worden pushmeldingen tijdens de overdracht end-to-end gecodeerd, waardoor organisaties meer controle hebben over de verwerking van mobiele gegevens.
- X Model met minimale machtigingen:** uitsluitend app-verzoeken.
- X Beperkte toegang tot apparaatfuncties** . Ondersteunt leeftijdsverificatie en toont beleid bij de eerste opstart.

De app is ontwikkeld om uw Moodle-site uit te breiden, niet te beperken. De app biedt gebruikers flexibiliteit en volledige controle over het gegevensgedrag op mobiele apparaten.

Vooruitzicht: een wereldwijd perspectief op leren en dataprotectie

Het recht op privacy is meer dan een afvinklijst in een beleidskader – het is een fundament van waardigheid, autonomie en vertrouwen in het digitale tijdperk. Wereldwijd heroverwogen wetgevers, instellingen en burgers de manieren waarop data worden verzameld, gebruikt en beschermd. Deze verschuiving is met name van groot belang in leeromgevingen, waar data vaak niet alleen weergeven wat mensen weten, maar ook wie ze zijn.

Bij Moodle zijn we van mening dat onderwijstechnologie moet voldoen aan de hoogste normen op het gebied van privacy. Dit is niet alleen wettelijk verplicht, maar ook de juiste benadering.



Afstemming op mondiale rechtenkaders

De open architectuur en de gebruikersgerichte filosofie van Moodle sluiten perfect aan bij internationale raamwerken zoals:

X AVG (EU): nadruk op gegevensminimalisatie, transparantie en individuele rechten.

X FERPA (VS): bescherming van de vertrouwelijkheid van studenten dossiers.

X POPIA (Zuid-Afrika) en LGPD (Brazilië): Toepassing gelocaliseerde privacyverklaring.

X Het VN-Verdrag betreffende de Rechten van het Kind: Het bevestigen van de rechten van kinderen op digitale privacy en bescherming.

Door tools te ontwikkelen die mensen meer mogelijkheden bieden in plaats van deze te ontnemen, ondersteunt Moodle organisaties in alle sectoren bij het handhaven van deze kaders en het tegelijkertijd inspelen op lokale behoeften en regelgeving.

Van naleving naar ethisch leiderschap

Nu de druk op platforms om verbeteringen door te voeren toeneemt, biedt het model van Moodle – geworteld in openheid, autonomie en ethische dienstverlening – een vooruitzicht. Onze gemeenschap reageert niet alleen op nalevingsvereisten, maar leidt ook gesprekken over **ethisch databeheer** in het onderwijs, de ontwikkeling van personeel en openbare trainingen.

Moodle-sites in het hoger onderwijs, het bedrijfsleven en de overheid demonstreren dat het mogelijk is om leer-ecosystemen te creëren die krachtig, schaalbaar en privacy-respectvol zijn, zonder in te boeten op bruikbaarheid, prestaties of betrouwbaarheid.

Onze toewijding

Wij blijven onze producten ontwikkelen met privacy als uitgangspunt, om te voldoen aan lokale behoeften en tegelijkertijd wereldwijde waarden te waarborgen. Wij pleiten voor meer transparantie en controle binnen het landschap van leertechnologie. Tevens blijven wij samenwerken met onze gemeenschap, partners en klanten om te garanderen dat de toekomst van leren niet alleen effectief is, maar ook respectvol, verantwoord en rechtvaardig.

**Omdat dataprivacy niet slechts een functie is.
Het is een fundament.**



Klaar om de volgende stap te maken?

Of je nu de naleving van regelgeving wilt versterken, gegevensbeheer wilt verbeteren of de beste praktijken op gebied van privacy wilt implementeren, als Moodle Certified Partner helpen we je graag!

Ontvang professionele ondersteuning die is afgestemd op de behoeften van jouw organisatie, zodat je met vertrouwen betrouwbare, privacygerichte leerervaringen kunt bieden.

[Neem vandaag
contact op](#)