Bijlage 2: Beveiligingsbijlage

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

1. Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

Momento hanteert een autorisatiebeleid, waardoor medewerkers op grond van dit beleid geen toegang hebben tot meer data dan strikt noodzakelijk is voor hun functie.

Medewerkers en gegevens:	Handelingen:
Medewerkers van de centrale helpdesk hebben toegang tot de volgende informatie: • BRIN van de onderwijsinstelling, • contactgegevens van de onderwijsinstelling (naam, straat, postcode, plaats), • contactgegevens van de ICT-coördinator die Momento heeft geactiveerd en namens de onderwijsinstelling de voorwaarden heeft geaccepteerd (naam, e-mailadres), • datum laatste synchronisatie schoolgegevens met Basispoort, • autorisatiesleutel waarmee bij uitgeverijen toestemming kan worden gegeven voor het opsturen van toetsresultaten, • uitgeverijen waarbij Momento resultaten van verwerken en oefenen mag ophalen, • probleemmeldingen in de logfiles, • datum laatste uitwisseling resultaten met uitgeverijen De medewerkers van de helpdesk klantenservice hebben geen inzage in licenties van leveranciers van leermiddelen of netwerkomgevingen van onderwijsinstellingen noch in leerresultaten van leerlingen, tenzij de helpdeskmedewerker in opdracht van de gebruiker een “meekijksessie” opstart. Zo’n sessie wordt vastgelegd in het registratiesysteem van de helpdesk.	De handelingen van helpdeskmedewerkers bestaan uit het ondersteunen van leerkrachten en onderwijsondersteunende medewerkers van een onderwijsinstelling in het kader van het inrichten en gebruiken van de aangeboden dienstverlening van Momento.
IT-databasebeheerders hebben toegang tot de databases.	De handelingen van IT-databasebeheerders zijn gericht op continuïteit en optimalisatie van ICT-systemen. Alleen op specifieke aanvraag mogen zij de database raadplegen en indien nodig vooraf gedefinieerde aanpassingen doorvoeren.

2. Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang of openbaarmaking.

Organisatie van informatiebeveiliging en communicatieprocessen

- Momento beschikt over een actief informatiebeveiligingsbeleid.
- Momento heeft een coördinator voor informatiebeveiliging in de persoon van de technisch projectleider, alsmede een Functionaris Gegevensbescherming. Zij inventariseren risico’s omtrent de verwerking van persoonsgegevens, stimuleren het beveiligingsbewustzijn, controleren voorzieningen en treffen maatregelen die zien op naleving van het informatiebeveiligingsbeleid.

- Informatiebeveiligingsincidenten worden gedocumenteerd in een overzicht/register en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Momento heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers
- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Momento stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.
- Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

3. Beveiliging en continuïteit van de middelen, het netwerk, de server en de applicatie

Momento heeft het Certificeringsschema (zie https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/) gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor de dienstverlening van Momento. Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

Toetsvorm	Self-assessment		
Uitvoerder toets	Momento: Marcel van der Veldt & Richard Hagen		
BIV-classificatie	Beschikbaarheid=3, Integriteit=2, Vertrouwelijkheid=2		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
Beschikbaarheid	Overbelasting	Voldaan	
	Business continuity	Voldaan	
	Ontwerp	Voldaan	
	Monitoring	Voldaan	
	Testen	Voldaan	
	Software	Voldaan	
	Actuele dreigingen	Voldaan	
Integriteit	Herleidbaarheid (gebruikers)	Voldaan	
	Backup	Voldaan	
	Application controls	Voldaan	
	Onweerlegbaarheid	Voldaan	
	Herleidbaarheid (technisch beheer)	Voldaan	
	Controle integriteit	Voldaan	
	Onweerlegbaarheid	Voldaan	
	Actuele dreigingen	Voldaan	
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	
	Logische toegang	Voldaan	
	Fysieke toegang	Voldaan	
	Netwerk toegang	Voldaan	
	Scheiding omgevingen	Voldaan	
	Transport en fysieke opslag	Voldaan	
	Logging	Voldaan	
	Toetsing	Voldaan	

	Actuele dreigingen	Voldaan	

Omschrijving van de maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

De systemen van **Momento** worden jaarlijks, of vaker indien daar, door bijvoorbeeld wijzigingen, aanleiding toe is, gecontroleerd op veiligheid door de bedrijven Computest https://www.computest.nl/ of Whitehats https://www.whitehats.nl/. Daarnaast voorziet het beveiligingsbeleid van **Momento** in interne processen om kwetsbaarheden te identificeren.

Rapportage

Verwerker actualiseert deze informatie indien daar aanleiding toe is en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via het onderdeel 'privacy' in het helpmenu van de applicatie en op de informatiesite www.momento.nl/privacy, waar ook deze bijlage (met technische en organisatorische beveiligingsmaatregelen) wordt gepubliceerd. In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van Momento via **088-4101060** of info@momento.nl.

Informeren over datalekken en/of incidenten met betrekking tot beveiliging

De wijze waarop monitoring en identificatie van Datalekken plaatsvindt

Momento monitort 24/7 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 de coördinator Informatiebeveiliging van Momento, die analyseert of sprake kan zijn van een datalek.

De wijze waarop informatie wordt gedeeld

Wanneer zich een datalek voordoet, wordt de daarbij getroffen verwerkersverantwoordelijke onderwijsinstelling door of namens Momento in beginsel zonder onredelijke vertraging na vaststelling geïnformeerd. Afhankelijk van de situatie, kan ook informatie worden gedeeld via onze website en officiële sociale media kanalen en/of officiële sub-verwerkers. Voor vervolgacties of vragen, kan telefonisch of per e-mail contact worden opgenomen met de helpdesk van Momento via 088-4101060 of help@momento.nl

Momento 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, waaronder toegangs- of identificatiegegevens).

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

Versie

Deze beveiligingsbijlage is voor het laatst bijgewerkt op 15 oktober 2021.