Bijlage 3 Beveiligingsbijlage DHH

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

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

Kwest Onderwijs hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

Hieronder wordt uitgewerkt welke (groepen) medewerkers van de Bewerker toegang hebben tot welke Persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers uit mogen voeren met de persoonsgegevens.

Groepen van medewerkers en Persoonsgegevens:	**Handelingen:**
Eerstelijns helpdesk, medewerkers van een eerstelijns helpdesk fungeren als aanspreekpunt. Ze beantwoorden 'basisvragen', verwijzen mensen door en maken indien nodig melding van inhoudelijke vragen of incidenten met indien relevant de desbetreffende leerling.	Ondersteuning van de eindgebruiker.
Tweedelijns helpdesk, medewerkers van een tweedelijns helpdesk beantwoorden zowel basis- als inhoudelijke vragen, analyseren incidenten (leerlinggegevens) en lossen op en koppelen dat ook weer terug naar de melder.	Ondersteuning van de eindgebruiker en na toestemming verdere ondersteuning met inzage of analyseren van het incident
Derdelijns support, medewerkers van derdelijns support zijn de experts en/of de ontwikkelaar van de applicatie. Zij ondersteunen bij het analyseren van incidenten (leerlinggegevens) en het oplossen en koppelen dat ook weer terug aan de tweedelijns Helpdesk	Analyseren van het incident
Analisten / deskundigen op het gebied van ontwikkeling van het product hebben toegang tot geanonimiseerde sets van resultaten van gebruik van het product, eventuele problemen/fouten bij gebruik IT-databasebeheerders hebben toegang tot de databases.	Analyse van het gebruik, gericht op verbetering van de functionaliteit, ontwikkeling en optimalisatie van, opsporing en verbetering van fouten in de werking van het product De handelingen van IT-databasebeheerders zijn gericht op continuïteit en optimalisatie van ICT-systemen.

II. 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.

Verwerker heeft het Certificeringsschema van Edu-K gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor WMK. 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		Kwest Onderwijs, H.T.F. Holtmaat coördinator informatiebeveiliging	
BIV-classificatie		[Beschikbaarheid=2, Integriteit=2, Vertrouwelijkheid=2]	
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
		[Voldaan/ niet voldaan/ alternatieve maatregel]	Bij niet voldaan aangeven hoe/wanneer dit wordt gecorrigeerd. Bij alternatieve maatregel deze beschrijven]
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**	
	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**	

Organisatie van informatiebeveiliging en communicatieprocessen

- Verwerker beschikt over een actief informatiebeveiligingsbeleid
- Verwerker heeft een coördinator voor informatiebeveiliging (security officer) 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.
- Verwerker heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

III. 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 Verwerker worden periodiek gecontroleerd op informatiebeveiliging door Kwest Onderwijs. Daarnaast voorziet het beveiligingsbeleid van Verwerker in interne processen om kwetsbaarheden te identificeren.

Rapportage

Verwerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via het onderdeel 'privacy' binnen de applicatie. In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van Verwerker via 0528-714301 of helpdesk@wmkpo.nl.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

De wijze waarop monitoring en identificatie van Datalekken plaatsvindt
Verwerker monitort 24/7 haar dienstverlening en heeft de in Bijlage 2 opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren. Signalen die duiden op een Datalek worden beoordeeld door de security officer van Verwerker, die analyseert of sprake kan zijn van een Datalek.

De wijze waarop informatie wordt gedeeld:
Wanneer zich een Datalek voordoet, wordt de Verwerkingsverantwoordelijke organisatie door of namens Verwerker in beginsel binnen binnen 24 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 0528-714301 of helpdesk@wmkpo.nl.

Verwerker 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).

Indien een concrete situatie zich daartoe leent, dan kan Verwerker 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.

Versie
Deze bijlage is voor het laatst bijgewerkt op 23 mei 2018.