Bijlage 2. Passende technische en organisatorische maatregelen

Bijlage 2: Beschrijving technische en organisatorische maatregelen (beveiligingsmaatregelen)

Waar van toepassing gedifferentieerd op basis van gevoeligheid van de in Bijlage 1 genoemde (categorieën) Persoonsgegevens.

Toepasselijke betrouwbaarheidseisen

Verwerkingsverantwoordelijke stelt hieronder vast aan welke eisen betreffende beschikbaarheid, integriteit en vertrouwelijkheid ter zake van de gegevensverwerking voldaan dient te worden. Met inachtneming van de onderstaande eisen draagt Dienstverlener ervoor zorg dat er sprake is van een passend beveiligingsniveau. Hierbij wordt in elk geval ISO 27001:2013 en/of NEN 7510:2011 als uitgangspunt genomen.

	Laag	Midden	Hoog
Beschikbaarheid			X
Integriteit			X
Vertrouwelijkheid			X

Uitwerking daarvan in concrete technische en organisatorische maatregelen

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

5.1.2.i 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.

Medewerkers en gegevens:	Handelingen:
Medewerkers van de klantenservice en 1ste-, 2de en 3e lijns helpdesk hebben op netwerkniveau toegang tot de verwerkingsomgeving. Zij hebben regulier geen inzage in persoonsgegevens. Wel nemen zij in voorkomende situaties systemen over dan wel loggen in binnen de applicatie met ter beschikking inloggegevens.	Administratieve handelingen in het kader van de werking van de netwerkomgeving en de infrastructuur. Ondersteuning van de eindgebruiker.
IT-beheerders hebben toegang tot de netwerkomgeving en de infrastructuur.	De handelingen van IT-beheerders 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.

1.1 Organisatie van informatiebeveiliging en communicatieprocessen

- 5.1.2.i 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.
- 5.1.2.i heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

1.2 Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- 5.1.2.i 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.
- Medewerkers betrokken bij onze dienstverlening beschikken over een recente Verklaring omtrent het Gedrag: dit wordt als eis bij indiensttreding opgelegd en specifieke gecontroleerd door de Security Officer. Elke 5 jaar wordt betreffende VOG opnieuw aangevraagd.

1.3 Fysieke beveiliging en continuïteit van de middelen

- 5.1.2.i

1.4 Netwerk-, server- en applicatiebeveiliging en onderhoud

- 5.1.2.i

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[5.1.2.i] . worden periodiek gecontroleerd op veiligheid door een extern bedrijf wat is gespecialiseerd in cybersecurity. Daarnaast voorziet het beveiligingsbeleid van[5.1.2.i] in interne processen om kwetsbaarheden te identificeren.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Met betrekking tot de meldplicht bij inbreuken in verband met Persoonsgegevens worden tussen Partijen de volgende afspraken gemaakt:

1. Verwerker registreert alle beveiligingsincidenten die verband houden met inbreuken op Persoonsgegevens.

2. Verwerker hanteert in de interne organisatie een “protocol datalekken”.

3. Indien Verwerker dan wel Verwerkingsverantwoordelijk een inbreuk in verband met Persoonsgegevens vaststelt, zal deze de andere Partij daarover zonder onredelijke vertraging informeren zodra zij kennis heeft genomen van de betreffende inbreuk. Verwerker informeert Verwerkingsverantwoordelijke in ieder geval binnen 8 uur.

4. Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Verwerker heeft geïnformeerd gemeld moet worden aan de AP en/of Betrokkene. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 Avg moeten worden gemeld aan de Autoriteit Persoonsgegevens en/of Betrokkene, blijft te allen tijde de verantwoordelijkheid van de Verwerkingsverantwoordelijke. Verwerker is niet verplicht tot het melden van inbreuken in verband met Persoonsgegevens aan de Autoriteit Persoonsgegevens en/of Betrokkene.

5. Verwerker verstrekt ingeval van een inbreuk alle relevante informatie aan Verwerkings-verantwoordelijke met betrekking tot de inbreuk, waaronder in ieder geval informatie over:
   - De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident;
   - De (mogelijke) oorzaak van het beveiligingsincident;
   - De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;

6. Verwerker informeert Verwerkingsverantwoordelijke onverwijld indien een vermoeden bestaat dat de inbreuk in verband met Persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen zoals bedoeld in artikel 34 lid 1 AVG.

7. Verwerkingsverantwoordelijke wordt door Verwerker telefonisch en per mail geïnformeerd over de inbreuk met betrekking tot de persoonsgegevens op onderstaand telefoonnummer en e-mailadres. De betreffende gegevens worden aangeleverd door Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke staat er voor in dat de door hem verstrekte gegevens correct en volledig zijn. Verwerker is niet aansprakelijk voor schade die bij Verwerkingsverantwoordelijke ontstaat doordat deze als gevolg van onjuiste gegevens niet of niet tijdig is geïnformeerd over de betreffende inbreuk.