

Verwerkersovereenkomst 4.1_V1.5 - Stichting Basispoort

Bijlage 2 - Beveiligingsbijlage Basispoort

Dit is Beveiligingsbijlage 4.1_V1.10 van Stichting Basispoort (kvk 30260618).

Dit document is voor het laatst gewijzigd en gevalideerd op 3 juli 2025. Document is herzien op basis van de Model overeenkomst Edu-V Afsprakenstelsel. Verwijzingen naar Privacy Convenant zijn verdwenen. Verwijzingen naar Edu-V Afsprakenstelsel zijn toegevoegd. Inhoudelijk is er niets veranderd.

Voor de overeenkomst en alle bijlagen bij deze overeenkomst is gebruik gemaakt van de model Verwerkersovereenkomst 4.1 van het Edu-V Afsprakenstelsel.

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 van de Model Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

A. 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:

- Stichting Basispoort hanteert een actief en passend informatiebeveiligingsbeleid dat periodiek wordt geëvalueerd en - zo nodig - aangepast'.
- Stichting Basispoort heeft een coördinator voor informatiebeveiliging in de persoon van de technisch projectleider, alsmede een Functionaris Gegevensverwerking, aangemeld bij het Register FG's van de Autoriteit Persoonsgegevens, 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 informatie-beveiligingsbeleid.
- Informatiebeveiligingsincidenten/-inbreuken worden gedocumenteerd in een overzicht/register en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Stichting Basispoort heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten/-inbreuken.
- Stichting Basispoort laat jaarlijks informatiebeveiligingstesten uitvoeren.
- Stichting Basispoort heeft al haar dataverkeer en data 'at rest' versleuteld.

Medewerkers:

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Stichting Basispoort 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.

Leveranciers:

- Met leveranciers zijn verwerkersovereenkomsten afgesloten; zij zijn op de hoogte van de informatiebeveiligingseisen van Basispoort

B. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen.

Stichting Basispoort heeft het Certificeringsschema* gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor de Single-Sign-On-toegangsdienst van Basispoort. Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

*Zie https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/

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

Toetsvorm	Self-assessment		
Uitvoerder toets	Stichting Basispoort, Edwin Kense, coördinator informatiebeveiliging		
Inlogpagina	Medewerkers loggen altijd in via: https://www.basispoort.nl/login/medewerkers/ Onderwijsdeelnemers loggen op school in met een snelkoppeling op het bureaublad en een wachtwoord in de vorm van een plaatje of pincode. Onderwijsdeelnemers loggen buiten school in via: https://www.basispoort.nl/login/thuisgebruikers		
BIV-classificatie	Beschikbaarheid = 3 (hoog), Integriteit = 2 (middel), Vertrouwelijkheid = 2 (middel)		
Categorie	Maatregelen	Compliance	Uitleg indien niet voldaan
Beschikbaarheid	Ontwerp	Voldoen we aan	
	Capaciteit beheer	Voldoen we aan	
	Onderhoud	Voldoen we aan	
	Testen	Voldoen we aan	Performance-testen vinden alleen plaats bij fundamentele aanpassingen; niet bij reguliere jaarreleases.
	Monitoring	Voldoen we aan	
	Herstel	Alternatieve maatregel	Hosting bij Azure. Hierbij is de software automatisch verdeeld over meerdere servers, voorzien van failover-functionaliteit. Aanvullend vindt er een hot back-up plaats op een andere locatie. Recoverytesten worden NIET uitgevoerd.
Integriteit	Herleidbaarheid (gebruikers)	Voldoen we aan	
	Backup	Voldoen we aan	
	Application controls	Voldoen we aan	
	Onweerlegbaarheid	Voldoen we aan	
	Herleidbaarheid (technisch beheer)	Voldoen we aan	
	Controle integriteit	Voldoen we aan	Logtermijn is korter dan 13 maanden. Dit is beschreven in de Verwerkersovereenkomst.
	Onweerlegbaarheid (toepassing)	Voldoen we aan	

Vertrouwelijkheid	Levenscyclus gegevens	Voldoen we aan	
	Logische toegang	Voldoen we aan	Twee-factor-authenticatie is ingericht voor beheerders op de applicatie.
	Fysieke toegang	Voldoen we aan	
	Netwerk toegang	Voldoen we aan	
	Scheiding omgevingen	Voldoen we aan	
	Transport en fysieke opslag	Voldoen we aan	
	Logging	Voldoen we aan	
	Omgaan met kwetsbaarheden	Voldoen we aan	

C. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken.

De wijze waarop monitoring en identificatie van Datalekken plaatsvindt

Stichting Basispoort monitort 24/7 haar dienstverlening en heeft de in Bijlage 2 opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens (inbreuk) te voorkomen en te identificeren. Signalen die duiden op een inbreuk worden beoordeeld door de Coördinator Informatiebeveiliging van Stichting Basispoort, die analyseert of sprake kan zijn van een Datalek.

De wijze waarop informatie wordt gedeeld:

Wanneer zich een Datalek voordoet zal Stichting Basispoort met de Verwerkersverantwoordelijke onderwijsinstelling in beginsel zonder onredelijke vertraging in overleg treden, na vaststelling dat sprake is van een Datalek. Afhankelijk van de situatie, kan ook informatie worden gedeeld via onze website en officiële sociale media kanalen en/of officiële Sub-verwerkers. Voor vervolgvragen of vragen kan telefonisch of per e-mail contact worden opgenomen met De Basispoort helpdesk waarvan de contactgegevens hieronder staan vermeld, alsmede in bijlage 1 bij de Verwerkersovereenkomst.

Stichting Basispoort deelt ten minste de volgende informatie wanneer zich een Datalek voordoet:

- De kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk; samenvatting van de inbreuk, waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op welk onderdeel van de beveiliging heeft het betrekking, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van Persoonsgegevens;
- Of de bij de inbreuk betrokken Persoonsgegevens versleuteld, gehasht waren;
- De oorzaak van de inbreuk;
- De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
- Benoemen van betrokkenen die gevolgen kunnen ondervinden van de inbreuk, en de mate waarin;
- De omvang van de groep betrokkenen;
- Het soort gegevens dat door de inbreuk wordt getroffen (met name bijzondere gegevens, waaronder toegangs- of identificatiegegevens).

Indien een concrete situatie zich daartoe leent, dan kan Stichting Basispoort 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.

Rapportage

- Verwerker actualiseert informatie m.b.t. data-beveiliging voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via de startpagina op www.basispoort.nl en de informatiesite <https://info.basispoort.nl>. In het geval een gebruiker (meent) een beveiligingsrisico te constateren, dan wordt deze gebruiker verzocht direct contact op te nemen met de helpdesk van Stichting Basispoort (kvk: 30260618); telefonisch via 073 6287557 of per mail via info@basispoort.nl

Contact

In geval van een (vermoeden van een) inbreuk, beveiligingsincident en/of Datalek, kunnen de onderwijsinstelling en Verwerker in beginsel contact opnemen via e-mail of telefoon.

Secretaris van het dagelijks bestuur van de Stichting Basispoort (Jan Willem Besteman): info@basispoort.nl

De **Basispoort helpdesk**: 073 6287557 of help@basispoort.nl

Deze Beveiligingsbijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad, de verschillende betrokken ketenpartijen: MEVW (voorheen GEU), KBb-E, VDOD, Vereniging ExSamen en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <https://www.privacyconvenant.nl/>