Privacyreglement

BIJLAGE I Register van verwerkingsactiviteiten

BIJLAGE VIII Passende technische en organisatorische maatregelen

*De schoolleiding van Het Amsterdams Lyceum heeft op grond van haar bevoegdheid ex art. 5 lid 4 van het Managementstatuut op 1 augustus 2018 de hierna volgende **BIJLAGES I en VIII** bij het **Privacyreglement** vastgesteld na voorafgaande instemming van de afzonderlijke personeels- ouder- en leerlinggeledingen van de Medezeggenschapsraad o.g.v artt. 12 lid 1 sub m en n, 14 lid 2 sub f, respectievelijk 14 lid 3 sub d van de Wet medezeggenschap op scholen. De in bijlages opgenomen regelingen worden van kracht op de dag van vaststelling.*

BIJLAGE I van het Privacyreglement van Het Amsterdams Lyceum:

Register van verwerkingsactiviteiten

*Het feitelijke **Register** bestaat uit een Excelbestand en is niet in deze uitgave opgenomen. Het format en de hieronder beschreven wijze van inrichting van het Register maken deel uit van BIJLAGE I van het Privacyreglement van Het Amsterdams Lyceum.*
*Dit feitelijke **Register** wordt bewaard aan het adres van de school en is daar voor bevoegden ter inzage.*

Toelichting

Artikel 1

De Verordening verplicht de verwerkingsverantwoordelijke om een *Register van verwerkingsactiviteiten* bij te houden (artikel 30 AVG). In dit register moet worden aangetekend van welke categorieën betrokkenen gegevens worden verwerkt, om welk soort persoonsgegevens het gaat en voor welk doel dit plaatsvindt. Met dit register toont de verwerkingsverantwoordelijke aan dat de AVG wordt nageleefd.

Artikel 2

Deze BIJLAGE I bestaat uit vier documenten. Gezamenlijk vormen deze documenten het *Register van verwerkingsactiviteiten*.

Document 1 is een Excel format met per categorie van betrokkenen (leerlingen/personeel/etc.) een schematische weergave van persoonsgegevens gekoppeld aan de doelen waarvoor zij worden verwerkt. Per koppeling kan in dit document worden bijgehouden:

- de interne en externe ontvangers (verwerkers) van de persoonsgegevens;
- de bewaartermijn;
- een risicoclassificering (Intern c.q. openbaar/vertrouwelijk/ geheim c.q. gevoelig);
- de herkomst van de gegevens; en
- de systeembron, met andere woorden: vindplaats c.q. bewaarplek van de gegevens.

Ook bevat het format (zoals door de AVG verplicht) een algemene beschrijving van de beveiligingsmaatregelen en wordt informatie geclassificeerd aan de hand van de kwaliteitscriteria Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

Document 2 (bijlage 1) omvat een overzicht van de door de verwerkingsverantwoordelijke concreet gehanteerde bewaartermijnen (dataminimalisatiebeleid) van onderliggende brondocumenten (de gegevensdragers).
Document 3 (bijlage 2) is een actueel overzicht van interne verwerkers die toegang hebben tot de persoonsgegevens en beschrijft 'wie heeft toegang tot welke gegevens'.
Document 4 (bijlage 3) voorziet in een overzicht van gegevensverwerkingen waarbij doorgifte aan derde landen of internationale organisaties plaatsvindt.

Artikel 3

Het format van het Register is opgesteld en ingevuld overeenkomstig de gegevensverwerkingen (soort gegevens en doel) zoals opgenomen in artikel 5 van het Privacyreglement. Voor wat betreft de bewaartermijnen en de interne ontvangers komen de in het format opgenomen informatie overeen met de gegevens in de hierna opgenomen bijlages 2 en 3.

Bijlage 1 Brondocumenten/brongegevens en bewaartermijnen

Deze bijlage bevat een overzicht van de van de door Het Amsterdams Lyceum gehanteerde bewaartermijnen ten aanzien van de brondocumenten en brongegevens die van toepassing zijn op de verwerkingen zoals opgenomen in het *Register van verwerkingsactiviteiten*, BIJLAGE I bij het Privacyreglement. Waar geen afwijkende termijn is ingevuld in de rubriek *Gehanteerde bewaartermijn*, is de termijn onder *Richtlijn bewaartermijn* van toepassing.

Categorie: leerlingen/oud-leerlingen (onderwijskundig)

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Het onderwijskundig rapport	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	
Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	
Gegevens over leerprestaties van de leerling	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	

Werk van het centraal examen en de rekentoets	minimaal 6 maanden (art. 57 Examenbesluit) Let op: verplichte wettelijke termijn!	na vaststelling van de uitslag	
Verslagen van gesprekken met de ouders	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	
Psychologisch rapport	maximaal 2 jaar Wanneer het rapport wordt opgevraagd bij een school voor po in het kader van toelating tot een school voor vo minimaal 3 en maximaal 5 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	
Adresgegevens	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	maximaal 6 maanden (art. 32 lid 6 en art. 34 lid 5 Vrijstellingsbesluit Wbp *oud*)	moment van opname	
[…]	[…]	[…]	

Categorie: leerlingen/oud-leerlingen (administratief)

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school ontvangt	minimaal 7 jaar (art. 103a lid 3 Wvo) Let op: verplichte wettelijke termijn!	na afloop van het schooljaar waarop de bekostiging betrekking heeft	
Gegevens over in- en uitschrijving	minimaal 5 jaar (art. 6 Bekostigingsbesluit Wvo) Let op: verplichte wettelijke termijn!	datum van uitschrijving	
Gegevens over verzuim en afwezigheid	minimaal 5 jaar (art. 6 Bekostigingsbesluit Wvo) Let op: verplichte wettelijke termijn!	datum van uitschrijving	

Gegevens met betrekking tot de vergoeding van de kosten verbonden aan leerlingvervoer	maximaal 2 jaar (art. 21 lid 5 Vrijstellingsbesluit Wbp *oud*)	na afloop van het schooljaar waarop de verstrekking van de vergoeding betrekking heeft	
Communicatiegegevens oud-leerlingen	Verwijderen op verzoek van de leerling of bij diens overlijden (art. 41 lid 5 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	
[…]	[…]	[…]	

Categorie: personeel/oud-medewerkers/leden toezichthoudend orgaan

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Akte van benoeming/ arbeidsovereenkomst	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Wijzigingen arbeidsovereenkomst	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Correspondentie inzake benoemingen, promotie, demotie	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Aanspraken in verband met de beëindiging van het dienstverband	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	datum waarop aanspraken zijn geëindigd	
Afspraken inzake werk MR	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde lidmaatschap	
Burgerlijke staat werknemer	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Kopie getuigschrift	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Afspraken inzake opleidingen	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Aanvraag opleiding door werknemer	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	

Afspraken omtrent loopbaan	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Verslagen functionerings- en beoordelingsgesprekken	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Correspondentie UWV en bedrijfsarts	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Verslaglegging inzake Wet Verbetering Poortwachter	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Verzuimregistratie als werkgever eigenrisicodrager Ziektewet is	minimaal 5 jaar De bedrijfsarts moet de gegevens minimaal 10 jaar bewaren. In verband met eigenrisicodragerschap WGA mogen de gegevens voor de duur van het WGA-traject bewaard blijven (10 jaar). (art. 3 lid 2 Regeling werkzaamheden, administratieve voorschriften en kosten eigenrisicodragen ZW) Let op: verplichte wettelijke termijn!	einde dienstverband	
Verslaglegging van correspondentie met betrekking tot problematische (financiële) privé-situatie	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Loonbeslagen	tot opheffing (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	-	
Correspondentie met betrekking tot jubilea	tot einde dienstverband (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	-	
Correspondentie directie/PZ/direct leidinggevende	afhankelijk van ontslagsituatie bij einde dienstverband of tot maximaal 2 jaar daarna (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	-	
Identiteitspapieren van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	minimaal 5 jaar (art. 15 lid 4 Wet arbeid vreemdelingen) Let op: verplichte wettelijke termijn!	einde dienstverband	

Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	maximaal twee jaar (art. 32 lid 6 en art. 34 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
Loonadministratie	minimaal 7 jaar (art. 52 lid 4 Algemene wet inzake rijksbelastingen) Let op: verplichte wettelijke termijn!	na afloop boekjaar	
Loonbelastingverklaringen en kopie identiteitsbewijs uit loonadministratie	minimaal 5 jaar (art. 7.5. lid 4 en art. 7.9. lid 2 Uitvoeringsregeling loonbelasting) Let op: verplichte wettelijke termijn!	na einde kalenderjaar waarin dienstverband is geëindigd	
Communicatiegegevens oud-personeelsleden	Verwijderen op verzoek van het oud-personeelslid of bij diens overlijden (art. 41 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	
[…]	[…]	[…]	

Categorie: sollicitanten

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Sollicitatiebrief, -formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant (art. 5 lid 6 en art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	na beëindiging sollicitatieprocedure of einde dienstverband/benoemings-termijn	
[…]	[…]	[…]	

Categorie: leveranciers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Persoonsgegevens van (vertegenwoordigers van) leveranciers	maximaal 2 jaar (art. 13 lid 5 Vrijstellingsbesluit Wbp *oud*)	nadat de desbetreffende transactie is afgewikkeld	
[…]	[…]	[…]	

Categorie: huurders / medegebruikers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Persoonsgegevens van huurders	maximaal 2 jaar (art. 14 lid 5 Vrijstellingsbesluit Wbp *oud*)	maximaal 2 jaar nadat de huur is beëindigd	
[…]	[…]	[…]	

Categorie: alle bovengenoemde categorieën en bezoekers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Camera en videobeelden	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten (art. 38 lid 6 Vrijstellingsbesluit Wbp *oud*)	moment van opname	
Gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de video-opnamen zijn gemaakt.	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten (art. 38 lid 6 Vrijstellingsbesluit Wbp *oud*)	moment van opname	
Registratielijsten bezoekers	niet langer dan nodig (art. 5 lid 1e AVG)	moment van registratie	

Toelichting bij bijlage 1

Deze bijlage voorziet in een model om bewaartermijnen van de documenten en gegevens in kaart te brengen die samenhangen met de verwerkingen zoals opgenomen in het Register. Het overzicht dient enerzijds als beleidsdocument om werkprocessen binnen de organisatie in overeenstemming te brengen met de verplichting om gegevens (aantoonbaar) niet langer te bewaren dan nodig is. Anderzijds vormt dit overzicht een handzaam document om te kunnen voldoen aan de verplichting om betrokkenen van wie persoonsgegevens worden verwerkt te informeren over de bewaartermijnen die de organisatie hanteert.

Hoofdregel

Volgens de AVG mogen persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor de gegevens zijn verzameld of worden gebruikt (art. 5 lid 1e AVG). Het is dus in beginsel aan de verwerkingsverantwoordelijke om aan de hand van het doel zoals omschreven in het Register van verwerkingsactiviteiten en artikel 5 van het reglement te bepalen hoelang gegevens worden bewaard (de gehanteerde termijnen).

Richtlijn bewaartermijn

Naast de hoofdregel dat persoonsgegevens niet langer mogen worden bewaard dan nodig, heeft de nationale wetgever voor enkele specifieke gegevens en brondocumenten in verschillende wetten al concrete bewaartermijnen gesteld. Deze termijnen zijn in kolom 2 opgenomen als richtlijn voor de te hanteren bewaartermijn. Vaak betreft dit een maximale bewaartermijn, in enkele gevallen schrijft de wet een minimale bewaartermijn voor. Dit betekent voor de verwerkingsverantwoordelijke dat zij ten aanzien van deze documenten naast haar eigen beoordeling, tevens is gebonden aan de minimale en maximale termijnen die uit de wet volgen.

In kolom 2 wordt regelmatig verwezen naar de inmiddels vervallen Wet bescherming persoonsgegevens (Wbp) en het daarbij horende Vrijstellingsbesluit. Hoewel deze wet en dit besluit niet meer van toepassing zijn, zijn de daarin opgenomen concrete bewaartermijnen onverminderd relevant. Bij de totstandkoming van de Wbp en het besluit heeft de wetgever destijds de afweging gemaakt die nu door de verwerkingsverantwoordelijke dient te worden gemaakt; hoelang is het nodig om de gegevens te bewaren met het oog op het doel waarvoor ze worden verzameld? Om deze reden kunnen ook deze inmiddels vervallen wettelijke termijnen dienen als richtlijn om de bewaartermijn vast te stellen. Soms wordt in kolom 2 verwezen naar een bewaartermijn uit een andere wet. Dit betreffen wettelijk termijnen (te herkennen aan: ‘Let op: verplichte wettelijke bewaartermijn!’). Ten aanzien van deze termijnen dient de verwerkingsverantwoordelijk zich ten minste te houden aan de gestelde minimale of maximale termijn uit de wet.

Bijlage 2 Overzicht van toegangsrechten interne verwerkers (ontvangers)

Overzicht van diegenen die toegang hebben tot de persoonsregistratie van de Het Amsterdams Lyceum zoals bedoeld in artikel 4 van het Privacyreglement:

Functie	Toegang tot welke persoonsgegevens
Schoolleiding	Alle gegevens van het personeel, sollicitanten, leerlingen en hun ouder(s)/verzorger(s), leden van het toezichthoudend orgaan en overig betrokkenen.
Functionaris gegevensbescherming	Alle gegevens van het personeel, sollicitanten, leerlingen en hun ouder(s)/verzorger(s), leden van het toezichthoudend orgaan en overige betrokkenen.
Incident Response team (IRT)	Alle gegevens van het personeel, sollicitanten, leerlingen en hun ouder(s)/verzorger(s), leden van het toezichthoudend orgaan en bezoekers.
Medewerkers administratie	Alle NAW-gegevens van het personeel, leerlingen en hun ouder(s)/verzorger(s), studieresultaten, aanwezigheidsregistratie, LVS.
Medewerkers HRM	Alle gegevens van het personeel en sollicitanten.
Medewerkers financiële administratie	Alle gegevens van het personeel die noodzakelijk zijn voor de uitvoering van de salarisadministratie, of voor de uitbetaling van gemaakte reiskosten van sollicitanten, NAW-gegevens van leerlingen en hun ouder(s)/verzorger(s).
Preventiemedewerker	Gegevens nodig voor het uitvoeren van de Arbowet, NAW-gegevens van het personeel.
Secretariaat	NAW-gegevens van personeel, leerlingen en hun ouder(s)/verzorger(s), cijfers, aanwezigheidsregistratie, LVS.
Applicatiebeheerder	Alle gegevens van het personeel, leerlingen en hun ouder(s)/verzorger(s), LVS voor zover noodzakelijk voor de uitvoering van de functie.
Decaan/studiecoördinator/mentor	Alle gegevens van leerlingen met wie ze vanuit hun functie een binding hebben, de NAW-gegevens van hun ouder(s)/verzorger(s), LVS.
Docenten/leraren	Alle gegevens van de leerlingen en de ouder(s)/verzorger(s) van de leerlingen aan wie zij lesgeven, cijfers, aanwezigheidsregistratie, LVS.
Leerlingen	De NAW-gegevens, behaalde cijfers en aanwezigheidsregistratie van de leerling zelf.
Ouders	De NAW-gegevens, behaalde cijfers en aanwezigheidsregistratie van de eigen kinderen tot de leeftijd van 18 jaar, de eigen persoonsgegevens.

Zorgverleners/zorgteam*	Alle gegevens van de leerlingen die extra zorg behoeven, de NAW-gegevens van de ouders(s)/verzorger(s) en de cijfers, aanwezigheidsregistratie en LVS.
Conciërges	De NAW-gegevens van personeel, leerlingen en ouder(s)/verzorger(s), afwezigheidsregistratie.
Afdelingsleiders	De gegevens van leerlingen en ouder(s)/verzorger(s) met wie ze vanuit hun functie een binding hebben, cijfers, aanwezigheidsregistratie en LVS.
Examensecretaris	NAW-gegevens van leerlingen, NAW-gegevens van hun ouder(s)/verzorger(s), cijfers, aanwezigheidsregistratie, LVS.
Mediatheekmedewerker	De NAW-gegevens van personeel, leerlingen en ouder(s)/verzorger(s).
Roostermakers	De NAW-gegevens van leerlingen en leraren, aanwezigheidsregistratie.
Verzuim coördinatoren	NAW-gegevens van leerlingen en hun ouder(s)/verzorger(s), aanwezigheidsregistratie en LVS.

** Let op: indien externe partijen (arts/schoolbegeleidingsdienst/orthopedagoog) deelnemen aan het zorgteam, dienen met deze partijen aparte afspraken te worden gemaakt.*

NAW-gegevens: een reeks van persoonsgegevens afgeleid van Naam, Adres en Woonplaats welke ook andere gegevens bevat.
LVS: leerlingvolgsysteem

Deze bijlage is voor het laatst gewijzigd op […].

Bijlage 3 Doorgifte aan derde landen en internationale organisaties

Overzicht van doorgiften van persoonsgegevens aan derde landen of internationale organisaties.

Omschrijving gegevensverwerking	**Doorgifte vindt plaats aan:** (land)

Deze bijlage is voor het laatst gewijzigd op […].

BIJLAGE VIII van het Privacyreglement van Het Amsterdams Lyceum:

Passende technische en organisatorische maatregelen

TOELICHTING

De AVG verplicht de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen die waarborgen dat de gegevens adequaat zijn beveiligd en gegevens beschermd zijn tegen ongeoorloofde verwerking en tegen verlies, vernietiging of beschadiging.

Normenkader informatiebeveiliging in het onderwijs

Kennisnet heeft de risico's in kaart gebracht die een rol spelen bij informatiebeveiliging binnen onderwijsinstellingen.[1] Deze risico's zijn vervolgens gekoppeld aan NEN- en ISO normen (het uitgangspunt als het gaat om de beveiliging van (persoons)gegevens) en door Kennisnet, SURF en saMBO-ICT voor het middelbaar beroepsonderwijs (mbo) vertaald in een 'normenkader'.[2]

Door de maatregelen uit dit normenkader na te leven is de onderwijsinstelling verzekerd dat zij haar persoonsgegevens adequaat heeft beveiligd. Dit normenkader is tevens bruikbaar voor het funderend onderwijs. Naar verwachting ontwikkelt Kennisnet op termijn ook voor het primair en voortgezet onderwijs een eigen variant.

Het normenkader is te onderscheiden in zes deelgebieden:

- het beleid met betrekking tot gegevensverwerkingen (organisatie);
- personeel, leerlingen en bezoekers;
- ruimtes en apparatuur;
- continuïteit;
- vertrouwelijkheid en integriteit;
- controle en logging.

---

1 https://www.sambo-ict.nl/wp-content/uploads/2017/09/IBPDOC29-Handleiding-Risico-management-versie-1.2.docx, bijlage 1: Overzicht risico's en maatregelen ISO27002/2013

2 https://www.sambo-ict.nl/wp-content/uploads/2015/02/IBBDOC2-Normenkader-Informatiebeveiliging-MBO-versie-1.0-Creative-Commons.pdf en https://www.nen.nl/NEN-Shop/Norm/NENENISOIEC-270012017-en.htm.

De maatregelen die de onderwijsinstelling dient te nemen op basis van dit normenkader zijn door Kennisnet beschreven en (één-op-één) overgenomen in de hieronder opgenomen **bijlage 1**. Voor zover de BIJLAGES bij het Privacyreglement hierin niet voorzien, zal nog uitvoering moeten worden gegeven aan (een deel van) de maatregelen en dient de onderwijsinstelling voor de maatregelen waar het handboek niet in voorziet aanvullend (en organisatie-specifiek) beleid te ontwikkelen. Op de punten waar aanvullend beleid nodig is wordt waar mogelijk verwezen naar bruikbare documenten van Kennisnet en saMBO-ICT.

Gegevensuitwisseling buiten de EU

Als persoonsgegevens worden doorgegeven aan een land buiten de Europese Economische Ruimte (EER) moet er sprake zijn van een beveiligingsniveau dat vergelijkbaar is met het beveiligingsniveau onder de AVG. Om dit te waarborgen zijn er de volgende mogelijkheden:

a) doorgifte op basis van een adequaatheidsbesluit van de Europese Commissie;
b) doorgifte op basis van passende waarborgen, wanneer een land of organisatie niet als adequaat is aangemerkt door de Europese Commissie kan doorgifte plaatsvinden als de verwerkersverantwoordelijke en de verwerker (aantoonbaar) voorzien in passende waarborgen en afdwingbare rechten en rechtsmiddelen voor betrokkene(n);
c) doorgifte op basis van uitdrukkelijke toestemming van de betrokkene waarbij de betrokkene geïnformeerd is over de risico's, of wanneer sprake is van een situatie van noodzaak.

Gegevensuitwisseling naar de VS

De Europese Commissie (EC) heeft een regeling vastgesteld voor doorgifte van persoonsgegevens aan de Verenigde Staten (VS). Deze regeling heet het EU-VS privacy shield (privacyschild). Het doel van het privacy shield is bij uitwisseling van persoonsgegevens met de VS een beschermingsniveau te bieden dat in grote lijnen overeenkomt met het niveau binnen de Europese Unie (EU). Het privacy shield komt in de plaats van de Safe Harbour-overeenkomst, die het Europees Hof van Justitie op 6 oktober 2015 ongeldig verklaarde. Elke organisatie in de VS die gecertificeerd is bij het privacy shield, heeft een passend beschermingsniveau (voor de duur van de certificatie). Dat betekent dat organisaties vanuit Europa persoonsgegevens mogen doorgeven naar deze organisaties inde VS.

Bijlage 1 Maatregelen voor informatiebeveiliging en bescherming van persoonsgegevens

Bron: IBPDOC2A Normenkader informatiebeveiliging MBO versie 2.0 zoals ontwikkeld door Kennisnet, SURF en saMBO-ICT

1. Beleid en organisatie

Maatregelen	Beleid
Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.	Reglement met BIJLAGEN
Het vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Privacyverklaring (art. 6.1 Privacyreglement) en BIJLAGE XIII (Handboek Datalekken)
Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Zie handboek saMBO-ICT: https://www.sambo-ict.nl/wp-content/uploads/2015/02/IBBDOC3-Handboek-MBOaudit-versie-1.1-Creative-Commons.pdf
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Benoemen FG, per functie verantwoordelijkheden vaststellen en opnemen in instructie aan personeel.
Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Zie handreiking door saMBO-ICT en Kennisnet: www.sambo-ict.nl/wp-content/uploads/2013/06/HoeZo-Bring-Your-Own-Device.pdf
Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	BIJLAGE I Register van Verwerkingsactiviteiten
Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	BIJLAGE I Register van Verwerkingsactiviteiten
Ter bescherming van informatie behoort een beleid voor het gebruik van crypto-grafische beheersmaatregelen te worden ontwikkeld.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto-grafische beheersmaatregelen wordt geïmplementeerd.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	BIJLAGE III Protocol gebruik e-mail, internet en sociale media

Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	BIJLAGE III Protocol gebruik e-mail, internet en sociale media
Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	BIJLAGE XI, BIJLAGE XII Verwerkersovereenkomst(en)
De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Door schoolleiding te beleggen indien aan de orde.
Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	BIJLAGE XI, BIJLAGE XII Verwerkersovereenkomst(en)
Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	BIJLAGE XI, BIJLAGE XII Verwerkersovereenkomst(en)
Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	BIJLAGE XIII Handboek Datalekken Zie ook het dossier DDoS-aanval op school in de aanpak IBP van Kennisnet: https://maken.wikiwijs.nl/81891/Aanpak_IBP_voor_het_PO_en_VO#!page-3692866
Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	BIJLAGE XIII Handboek Datalekken Zie ook het dossier DDoS-aanval op school in de aanpak IBP van Kennisnet: https://maken.wikiwijs.nl/81891/Aanpak_IBP_voor_het_PO_en_VO#!page-3692866
Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Privacyreglement met BIJLAGEN
Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Privacyreglement met BIJLAGEN
Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Inpassen in functiebouwwerk.

2. Personeel

Maatregelen	Beleid
De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	BIJLAGE V, Aanstellings- c.q. benoemingsbeleid
Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Scholingsagenda Zie de brochure ICT bekwaamheid door saMBO-ICT: https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/hoezo/Hoe_Zo_Ict-bekwaamheid_in_het_mbo.pdf
De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Autorisatiebeleid
Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.	Clear desk- en screenbeleid
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	Periodieke audit naleving AVG
Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	BIJLAGE III (Protocol e-mail, internet en sociale media) art. 5.3 en art. 4 van bijlage 1 (Protocol beveiligingsincidenten) bij BIJLAGE XIII (Handboek Datalekken).
Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	Aanstellings- c.q. benoemingsbeleid.

3. Ruimtes en apparatuur

Maatregelen	Beleid
Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.	BIJLAGE III - Protocol e-mail, internet en sociale media Zie handreiking door saMBO-ICT en Kennisnet: www.sambo-ict.nl/wp-content/uploads/2013/06/HoeZo-Bring-Your-Own-Device.pdf
Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Taak ICT-verantwoordelijke
Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	BIJLAGE I, bijlage 2, toegangsrechten informatie
Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	BIJLAGE I, bijlage 2, toegangsrechten informatie
Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Taak schoolleiding
Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Taak ICT-verantwoordelijke en schoolleiding
Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	Taak schoolleiding en BIJLAGE IV- Protocol camera- en videobeelden.
Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Taak ICT-verantwoordelijke en schoolleiding
Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Taakomschrijving ICT (intern dan wel extern te beleggen)

Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	BIJLAGE III - Protocol e-mail, internet en sociale media
Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	Taakomschrijving ICT (intern dan wel extern te beleggen)
De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	Taakomschrijving ICT (intern dan wel extern te beleggen)

4. Continuïteit

Maatregelen	Beleid
Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	BIJLAGE VI – Regeling taken en verantwoordelijkheden Functionaris Gegevensbescherming.
Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.	Scholingsagenda Zie de brochure ICT bekwaamheid door saMBO-ICT: https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/hoezo/Hoe_Zo_Ict-bekwaamheid_in_het_mbo.pdf
Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.	Back-up beleid
Gemaakte back ups worden regelmatig getest conform het back-up beleid.	Auditbeleid
Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	Taakomschrijving ICT (intern dan wel extern te beleggen)

Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	BIJLAGE VI - Regeling taken en verantwoordelijkheden Functionaris Gegevensbescherming BIJLAGE III (Protocol e-mail, internet en sociale media) art. 5.3 en bijlage 1 BIJLAGE XIII (Handboek Datalekken).
Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	BIJLAGE III Protocol e-mail, internet en sociale media
Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Gegevensbeschermingseffectbeoordeling BIJLAGEN XI en XII (Verwerkersovereenkomsten) Auditbeleid
Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten.	BIJLAGE XIII - Handboek Datalekken
Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	BIJLAGE XIII - Handboek Datalekken
De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Taakomschrijving ICT (intern dan wel extern te beleggen)

5. Vertrouwelijkheid en integriteit

Maatregelen	Beleid
Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Autorisatiebeleid
Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Autorisatiebeleid en BIJLAGE I - Register van verwerkingsactiviteiten
Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Autorisatiebeleid en BIJLAGE I - Register van verwerkingsactiviteiten
Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Autorisatiebeleid en BIJLAGE I - Register van verwerkingsactiviteiten
Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Autorisatiebeleid en BIJLAGE I - Register van verwerkingsactiviteiten
Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	Autorisatiebeleid en BIJLAGE I - Register van verwerkingsactiviteiten
Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.	BIJLAGE III - Protocol e-mail, internet en sociale media
Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	BIJLAGE I - Register van verwerkingsactiviteiten
Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Autorisatiebeleid
Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Taakomschrijving ICT (intern dan wel extern te beleggen)

Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	BIJLAGE XI, BIJLAGE XII - Verwerkersovereenkomsten
Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	BIJLAGE III - Protocol e-mail, internet en sociale media
Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Taakomschrijving ICT (intern dan wel extern te beleggen)

6. Controle en logging

Maatregelen	Beleid
Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Autorisatiebeleid
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Taakomschrijving ICT (intern dan wel extern te beleggen), BIJLAGE VI - Taken en verantwoordelijkheden FG
Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	BIJLAGE VI - Taken en verantwoordelijkheden FG
Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Taakomschrijving ICT (intern dan wel extern te beleggen)

Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	Auditbeleid
De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Taakomschrijving ICT (intern dan wel extern te beleggen)
Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	BIJLAGE VI - Taken en verantwoordelijkheden FG Auditbeleid
Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	BIJLAGE VI - Taken en verantwoordelijkheden FG Auditbeleid