Informatiebeveiligings- en privacy beleid – zijnde AVG-beleid

CBO De Greiden

Oktober 2020

1 Het belang van informatiebeveiliging en privacy

Het informatiebeveiligings- en privacy beleid is aangepast aan de eisen en termen vanuit de AVG. Elke organisatie moet niet alleen de privacy wetgeving naleven, maar moet ook aantoonbaar voldoen aan de AVG.
Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ict. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot AVG) in een AVG-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

Relatie met visie missie uit Strategisch Beleidsplan van De Greiden

DORST naar kennis en ontwikkeling
Ruimte voor (op)groeien in een veilige omgeving

In het strategisch beleidsplan gaan we ervan uit dat alle scholen van De Greiden voldoen aan de eisen die van overheidswege worden gesteld. Dit basisniveau borgen wij door vanuit het bestuur interne audits te plannen. Naast het borgen van het basisniveau worden in dialoog met de scholen onze ambities vorm gegeven. Al onze ambities zijn gericht op de brede ontwikkeling van ons zelf en onze leerlingen in samenhang met de wereld in een lerende organisatie.

Om onze ambities vorm te kunnen geven, kijken we naar onderwijs- en ondersteuningsbehoeftes. Deze manier van kijken en ondersteunen geldt voor alle niveaus: bij directeuren, bij leerkrachten en bij de leerlingen. Wij werken vanuit een veilig klimaat, waarin we ons blijven ontwikkelen, leren en waar fouten mogen worden gemaakt. Een deugdelijk en levend AVG-beleid is daarbij een belangrijke pijler voor veilig klimaat.

Wij gaan daarbij uit van vertrouwen. De basis is een veilige plek van waaruit de wereld kan worden ontdekt en vormgegeven, waar talenten van leerlingen en personeel worden ingezet en ontwikkeld om in te zetten voor zichzelf, voor anderen en voor de wereld met als doel dat we als mensheid met elkaar op de aarde kunnen samenleven.

De koers van CBO De Greiden:
De basisbehoeften: Relatie, Autonomie en Competentie staan centraal bij onze aanpak.

Vanuit een oprechte relatie geven we autonomie en bevorderen we de competenties.
We geloven in de samenwerking met de omgeving.
School en ouders werken constructief samen.
Ieder, vanuit de eigen rol, kan bijdragen aan een positieve ontwikkeling van het kind.

Respect is daarbij een basiswoord. Een veilig klimaat middels AVG een belangrijker pijler.

2 Toelichting informatiebeveiliging en privacy

Toelichting informatiebeveiliging
Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Toelichting privacy
Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Vervlechting informatiebeveiliging en privacy
Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: AVG. Dit beleid, verder te benoemen als AVG-beleid, vormt de basis op informatiebeveiliging en privacy binnen CBO De Greiden te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

Doel
Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan CBO De Greiden persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (AVG-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en CBO De Greiden voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het AVG-beleid binnen CBO De Greiden geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices (apparaten) van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het AVG-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen CBO De Greiden waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan CBO De Greiden persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van CBO De Greiden Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)

- Het AVG-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van CBO De Greiden evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het AVG-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- AVG-beleid heeft binnen CBO De Greiden raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
  - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
  - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

4 Beleid – Hoe doen we dat?

CBO De Greiden hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van CBO De Greiden neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

2. CBO De Greiden voldoet aan alle relevante wet- en regelgeving.

3. Bij CBO De Greiden is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van CBO De Greiden om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.

4. CBO De Greiden zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.

5. CBO De Greiden legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. CBO De Greiden voldoet hiermee aan de documentatieplicht.

6. Binnen CBO De Greiden is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten zoals de groepsmap en inschrijfformulieren. Het streven is om alle registratie op termijn te digitaliseren.

7. CBO De Greiden is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. CBO De Greiden classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de tenemen maatregelen.

9. CBO De Greiden sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

10. CBO De Greiden verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. CBO De Greiden heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij CBO De Greiden een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. CBO De Greiden kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. CBO De Greiden neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren. Berichten met bijzondere persoonsgegevens worden versleuteld verstuurd. Het streven is om in de toekomst dat bericht met bijzondere persoonsgegevens (te) delen ipv (te) mailen (delen betekent dat er in een systeem wordt ingelogd zoals Parnassys).

14. CBO De Greiden zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en indien nodig melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5 Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

Relevante wet- en regelgeving
De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

Basisregels bij het omgaan met persoonsgegevens
Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde AVG-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Ondersteunende richtlijnen en procedures
Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

Voorlichting en bewustzijn
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het AVG-bewustzijn is een gezamenlijke verantwoordelijkheid van het bestuur, schooldirecteuren, leerkrachten, overige medewerkers en de FG met het bestuur als eindverantwoordelijke.

Classificatie en risicoanalyse
Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

Incidenten en datalekken
Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij de schooldirecteur, daarna bestuur, daarna de FG.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

Planning en controle
Dit AVG-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geinventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent CBO De Greiden een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

Naleving en sancties
De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Elke proceseigenaar (medewerker) neemt zijn of haar verantwoordelijkheid. De direct leidinggevende spreekt een medewerker aan in geval van tekortkomingen. Er wordt actief aandacht besteed aan AVG bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan CBO De Greiden de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Logging en monitoring
Logging (registreren van handelingen in softwarepakketten die plaatsvinden) en monitoring door het externe ICT-bedrijf zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

6 Organisatie - Wie doet wat?

Rollen en verantwoordelijkheden

De organisatie van AVG gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht (met een niet limitatieve opsomming) geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij CBO De Greiden.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Strategisch	CvB	• Eindverantwoordelijk • AVG-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking AVG-beleid op basis van rapportages • Organisatie AVG inrichten	• Informatiebeveiligings- en privacy beleid • Basismaatregelen • Reglement FG • Privacyreglement • Gedragscode medewerkers en leerlingen • Verwerkersovereenkomsten
Tactisch	Schooldirecteur	• Inhoudelijk verantwoordelijk voor AVG • AVG-planning en controle • Adviseert CvB • Uitvoeren AVG-beleid, Classificatie/risicoanalyse (RIeE op AVG) • Voorbeeldfunctie met positieve en actieve houding t.a.v. AVG-beleid • Implementeren AVG-maatregelen • Periodiek het onderwerp informatiebeveiliging onder de aandacht brengen tijdens de gesprekkencyclus, werkoverleggen, beoordelingen, etc. • Rapporteren voortgang AVG in schooljaarverslag	• Uitvoeren jaarplan AVG • Uitvoering Protocol beveiligingsincidenten en datalekken • Aanvragen Verwerkingsovereenkomsten • Brief toestemming gebruik beeldmateriaal • Bewustwording • Sociale media reglement • Toezien op het naleven van gedragscodes • Toezien op de naleving van het delen van persoonsgegevens binnen en buiten de organisatie
	Functionaris voor Gegevensbescherming	• Toezicht op naleving privacywetgeving • Voorlichting privacy en stimuleren bewustwording • Aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement • Procedure AVG-incident afhandeling • Inrichten meldpunt datalekken • Overleg met CvB en werkgroep AVG
	Werkgroep AVG	• Advisering over privacyvraagstukken, AVG, werkprocessen, richtlijnen, bewustwording, etc. • AVG-beleid formuleren en monitoren • Schakel en klankbord tussen de werkvloer en het beleid	• De werkgroep komt meerdere keren per jaar bijeen en bestaat uit een afspiegeling van vertegenwoordiging van de organisatie (thans: CvB, GMR, directeur, FG)
Operationeel	Medewerker (OP en OOP)	• Uitvoeren taken conform AVG-beleid • Is verantwoordelijk voor de AVG in de dagelijkse werkzaamheden	• Naleving van het delen van persoonsgegevens binnen en buiten de organisatie volgens de gestelde richtlijnen • Naleven gedragscodes • Melden incidenten

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten: Aandachtspunten:

Nr	GMR	Omschrijving document	Jaar vaststelling
33041	*	Medewerker overeenkomst intern privacy en ICT-gebruikersbeleid	2019
33046		Data Protection Impact Assessment Externe verwerkers	2019
33050		Data Protection Impact Assessment organisatie	2019
33052		Data Protection Impact Assessment medewerkers	2019
33054	*	Privacyreglement leerlingen	2019
33055	*	Privacyreglement medewerker	2019
33056	*	Toestemming publicatie beeldmateriaal leerlingen	2019
33058	*	Sociale media reglement leerlingen	2019
33060	*	Sociale media reglement organisatie	2019
33064	*	Opgave verwerkte privacy- en persoonsgevoelige informatie leerlingen	2019
33065	*	Opgave verwerkte privacy- en persoonsgevoelige informatie medewerkers	2019
33066		Registratie en uitvoering cameratoezicht	2019
33067	*	Reglement cameratoezicht	2019
33068		Register van Verwerkingsactiviteiten	2019
33071		Privacy verklaring (website)	2019
33075	*	Toestemming publicatie persoonsgegevens medewerkers	2019
		Communicatie rechten betrokkenen (intern proces)–leerlingendossier	
		Autorisatiematrix	
		Wachtwoordbeleid (samen met gedragscode leerlingen,medewerkers)	Concept
		Gedragscode ict en internetgebruik	Concept
		Responsible disclosure (vgl. Kennisnet)	
		Gebruikersovereenkomst devices (ipad, pc, etc)	
		Procedure rondom uitwisselen gegevens (externe partijen)	
		Procesbeschrijving melden datalekken	
		Registratie beveiligingsincidenten	
		Registratie rechten betrokkenen (schoolniveau, verantwoording)	
		Risicoanalyse (BIV-classificatie)	
		Geheimhoudingsovereenkomst externe medewerkers (Intern beheer) https://aanpakibp.kennisnet.nl/gedragscode-veilig-gebruik-ict-middelen-en-persoonsgegevens/	Concept
		DPIA – kennisnet/sivon voor Parnassys	

Bijlage bewaartermijnen (obv leidende Archiefwet – kritisch volgen van Visma / Parnassys / Office 365 etc.)

Welke gegevens	Wettelijke basis	Uitleg	
1. Specifieke gevallen	specifieke wet	**Specifieke bewaar- c.q. vernietigingstermijn** terug te vinden in wet en regelgeving. Deze specifieke termijn wordt nagekomen. In de tabel in deze handreiking is een opsomming van specifieke bewaartermijnen te vinden (zie bijlage: lijst met termijnen in onderwijswetten).	
2. Europese subsidie (stimuleringsregeling)	ESF	Tot **10 jaar** na vertrek van de betreffende leerlingen/medewerkers moet informatie bewaard worden.	
3. Financiële en fiscale en bekostigingsbescheiden	Artikel 172 lid 3 Wet PO Artikel 130a lid 3 Wet VO	**7 jaar**	
4. Alle gegevens in de leerling administratie PO / VO	Artikel 9 lid 1 (juncto artikel 6 lid 1) bekostigingsbesluit WPO Artikel 6 bekostigingsbesluit VO	Tot **5 jaar** na uitschrijving betreffende leerling blijft diens informatie bewaard in de leerlingadministratie	
5. Persoonsgegevens betreffende de gezondheid van leerlingen	Artikel 18a lid 6 (juncto lod 13) Wet PO 17a lid 14 Wet VO	**3 jaar** na afloop van: (a.) de beoordeling of een leerling is aangewezen op het leerwegondersteunend onderwijs of van het toelaatbaar verklaren van leerlingen tot het praktijkonderwijs of het voortgezet speciaal onderwijs (b.) de advisering over de ondersteuningsbehoefte van de leerling aan het bevoegd gezag van de school, (c.) de toewijzing van ondersteuningsmiddelen of voorzieningen aan de school.	
6. Digitaal leermateriaal	Persoonsgegevens: niet langer bewaren dan noodzakelijk	Po Onderbouw vo	Gegevens huidige schooljaar, plus gegevens voorgaande schooljaar bewaren
		Bovenbouw vo	Gegevens huidige schooljaar, plus de twee voorgaande schooljaren bewaren
7. Alle andere gevallen	Gegevens tot personen herleidbaar	Vernietigen **2 jaar** na uitschrijven of beëindigen relatie	
	Toestemming om na uitschrijven gegevens te bewaren met specifiek doel	Bewaren toegestaan op basis van toestemming (bijv. alumni)	
	Niet tot persoon herleidbaar	Vrij te kiezen	

Bron schema:
https://aanpakibp.kennisnet.nl/app/uploads/Samenvatting-bewaartermijnen-1.1.pdf