Aandachtspunten AVG

Voldoen aan de AVG… wat moet ik nu regelen?

In Nederland wordt privacy beschermd door de Wet bescherming persoonsgegevens (Wbp). Op 25 mei 2018 wordt deze wet vervangen door een in heel Europa geldende verordening: een Europese wet die direct van toepassing is in alle landen van de Europese Unie.
In de basis verschilt de Wbp uit 2001 niet zoveel van de Algemene Verordening Gegevensbescherming (AVG). De AVG geeft **betrokkenen meer rechten** als het gaat om het verwerken van persoonsgegevens. Daarnaast wordt in de AVG **meer nadruk** gelegd op de **verantwoordelijkheid van organisaties** zelf om de wet na te leven, **transparant** te zijn over de omgang met persoonsgegeven én om te kunnen **aantonen** dat zij zich aan de wet houden.

Onderstaand overzicht is *geen checklist* die je afvinkt en vervolgens het voldoen aan de AVG voor altijd geregeld hebt. Voldoen aan de AVG is een continue proces waar je als school aan moet blijven werken. Eisen vanuit de AVG zijn vertaald naar aandachtspunten, waarbij is aangegeven wat een organisatie (voortdurend) moet regelen.

Ook onderwijsinstellingen in het po, vo en mbo moeten informatiebeveiliging en privacy (afgekort tot IBP) regelen. Naast de wettelijke verplichting vanuit de AVG zijn het ook belangrijke randvoorwaarden voor het gebruik van ict in het onderwijs.

Kennisnet, de PO-Raad en VO-raad helpen scholen om IBP goed en praktisch te regelen. Daartoe is een ‘kapstok’ ontwikkeld: de pragmatische **‘aanpak IBP’** helpt scholen om een (kort) beleid te maken, en op basis daarvan de nodige activiteiten te starten, maatregelen te nemen en afspraken vast te leggen.
De aanpak IBP bestaat, lekker eenvoudig, uit drie grote stappen: **organiseren** (schrijven van beleid), **realiseren** (activiteiten, documenten, afspraken met leveranciers) en **communiceren** (awareness en voorlichting voor leerlingen, medewerkers en ouders). De aanpak IBP bevat uitleg, voorbeelden en templates en gaat uit van de aandachtspunten van de AVG en internationale normen voor informatiebeveiliging (zoals de ISO 27001:2013). De aanpak IBP is te vinden via: https://kn.nu/IBPonderwijs.

De 'aandachtspunten AVG' gaan hierna in op de gevolgen die de uitgebreide (U) en nieuwe (N) regels van de AVG hebben voor jouw organisatie, wat je moet regelen en hoe de aanpak IBP je hierbij kan helpen.

Een aantal (complexe) handreikingen om te voldoen aan de AVG zijn op dit moment in ontwikkeling en worden in de loop van 2017 aan de Aanpak toegevoegd. Deze zijn in de laatste kolom in lichtgrijze tekst opgenomen. Een ‘procedure opstellen voor verwijderen van gegevens’, en ‘klachtenregistratie mogelijkheid’ staan niet in de aanpak. Dit zijn zodanig school specifieke onderwerpen dat organisaties daar zelf het initiatief in moeten nemen. Wel zijn deze onderwerpen vanuit de **aandachtspunten** AVG opgenomen in het overzicht.

* Nieuw
** Uitbreiding

AVG (en Wbp)	Omschrijving vanuit de wetgeving	N* U**	Wat is de praktijk	Wat moet ik regelen?	Waar te vinden in de Aanpak IBP
Uitgangspunten privacy *(Komen overeen met de bekende **5 vuistregels versie 2.0**)*					
☐ Doel en doelbinding	Persoonsgegevens mogen alleen verwerkt worden voor een vooraf vastgelegd doel. Er mag geen verdere verwerking van gegevens plaatsvinden als deze verwerking onverenigbaar is met het doel dat vooraf is vastgesteld	U	Doel en doelbinding is vastgesteld in het beleid en in privacyreglement. Art. 19 Vrijstellingsbesluit Wbp geeft toegestane doeleinden van verwerking voor scholen.	☐ AVG: vastleggen welke persoonsgegevens voor welke doelen gebruikt worden, hoe lang deze bewaard worden enz. *Zie ook Documentatieplicht*	Landelijk wordt er gewerkt aan een dataregister, dat het organisaties eenvoudiger moet maken om aan deze verplichting te voldoen
☐ Grondslag	Toestemming, overeenkomst, wettelijke plicht, uitvoeren publiekrechtelijke taak of gerechtvaardigd belang.	U	Verwerking vindt doorgaans plaats op basis van wet, wettelijke taak of gerechtvaardigd belang.	☐ Toestemming gebruik foto's en video's regelen.	Realiseren/aan de slag/ gebruik beeldmateriaal leerlingen

			Voor zover toestemming is vereist, moet die aantoonbaar zijn gegeven. Ook moet duidelijk zijn waarvoor de toestemming is gegeven	*Let OP: Niet alleen toestemming vragen, maar gegeven toestemming moet ook bewezen kunnen worden. Omgekeerde bewijslast is niet toegestaan (dus niet: 'u gaat akkoord tenzij…')*	
☐ Dataminimalisatie	Persoonsgegevens die verwerkt worden moeten redelijkerwijs nodig zijn om doel te bereiken (*proportioneel*). Doel kan niet met minder gegevens behaald worden (*subsidiair*)		Niet meer gegevens vragen dan strikt noodzakelijk en niet langer verwerken dan nodig om het doel te behalen. *Niet zo min mogelijk gegevens; wel alleen relevante gegevens*	☐ Leg bewaar- en vernietigtermijnen vast.	Landelijk wordt er gewerkt aan een dataregister, dat het organisaties eenvoudiger moet maken om aan deze verplichting te voldoen
				☐ Procedure opstellen voor verwijderen van gegevens	
☐ Transparantie	Transparantie en rechten betrokkenen: • Recht op informatie over gegevensverwerkingen **(U)** • Recht op inzage, correctie, verwijdering/afscherming en bezwaar (verzet) **(U)** • Recht om vergeten te worden (vergetelheid) **(N)** • Recht op dataportabiliteit **(N)** • Recht van informatie over en verzet tegen geautomatiseerde besluitvorming (profilering) **(N)** • Procedure rechten betrokkenen implementeren **(N)**	**U/N**	Alle betrokkene (leerling en/of ouders) moeten **vooraf in begrijpelijke taal geïnformeerd worden** over welke informatie voor welk doel verwerkt wordt en wat hun rechten en plichten zijn. Procedures zijn geregeld in het privacyreglement.	☐ Inzage en correctie procedure implementeren	Realiseren/aan de slag/rechten van betrokkenen procesbeschrijving rechten betrokkenen
				☐ Overzicht gebruikte gegevens	Landelijk wordt er gewerkt aan een dataregister, dat het organisaties eenvoudiger moet maken om aan deze verplichting te voldoen *(Zie ook documentatieplicht)*
				☐ Betrokkenen informeren over hun rechten	Realiseren/aan de slag/rechten van betrokkenen transparantie en rechten betrokkenen

				☐ Betrokkenen informeren over wat de school doet aan informatiebeveiliging en privacy	Realiseren/aan de slag/ privacyreglement en Realiseren/aan de slag/ Informatieplicht
				☐ Afspraken en procedures rondom privacy	Realiseren/aan de slag/ rechten van betrokkenen privacy afspraken en procedures
				☐ Klachtenregistratie mogelijkheid (klachtenformulier)	Zelf te regelen: registratie klachten en meldingen incidenten. (Kan aansluiten bij bestaande klachtenregistratie)
				☐ Beschikbaar stellen privacy bijsluiters (zie bewerkersovereenkomsten)	Realiseren/ aan de slag/ afspraken leveranciers
☐ Data-integriteit	Verwerkingen die door of namens de school gedaan worden moeten juist zijn en op het juiste moment op de juiste plaats aanwezig zijn. *Datakwaliteit en databeveiliging zijn hier van belang.*		De school moet passende technische en organisatorische maatregelen nemen.	☐ procedure opstellen voor inzage, correctie, verwijdering/ afscherming door betrokkenen	Een aantal adviezen staan in Realiseren/ aan de slag/ rechten van betrokkenen Privacy afspraken en procedures
				☐ toegangsmatrix opstellen	Hieraan wordt gewerkt en komt in de aanpak onder Realiseren/goed op weg/ Wie mogen gegevens inzien
				☐ regel afspraken rondom backup, antivirus enz	
				☐ Ingevoerde gegevens moeten juist (en gecontroleerd) zijn	

				☐ Gegevens zijn beschikbaar (continuïteit)	Afspraken over servicelevels met leveranciers maken
Privacy by design	Bij nieuwe verwerkingen/ ontwikkelingen moet vooraf aandacht besteed worden aan privacy verhogende maatregelen. *Vanaf het ontwerp moet er al aandacht zijn voor het goed*	**N**	Basis uitgangspunten privacy (5 vuistregels 2.0) toepassen vanaf de start van een project of wijziging van een applicatie waarbij persoonsgegevens verwerkt worden. Pas de regels ook toe op huidige situatie en bepaal met behulp	☐ Gegevensbeschermings-effectbeoordeling : vóóraf bij nieuwe ontwikkelingen; in ieder geval bij aankoop van (nieuwe) applicaties	Op dit moment wordt er gewerkt aan een format. voor een gegevensbeschermingseffectbeoordeling.
en **privacy by default**	*beveiligen van persoonsgegevens (zie uitgangspunten privacy).* ***NB**. De Autoriteit Persoonsgegevens komt met een lijst van met soorten verwerkingen waarbij een Gegevensbeschermingseffect-beoordeling verplicht is.* Uitgaan van standaardinstellingen, waarbij betrokkenen de keuze hebben om gegevens te delen of niet.	**N**	van een risico analyse de gewenste maatregelen om de risico's te verlagen. Standaardinstellingen vragen vervolgens om keuzes. Maak leerlingen, ouders en medewerkers bewust van de keuzes die ze hebben.	☐ Risico analyse (Breng de risico's in beeld van de huidige situatie en plan acties in)	Realiseren/classificeren en risicoanalyse Classificeren en risicoanalyse
				☐ Aandacht voor sociale media en mediawijsheid	Realiseren/goed op weg/ Afspraken over sociale media Maak leerlingen mediawijs
				☐ Aandacht voor ict bekwaamheid van medewerkers	Ict-bekwaamheid van de leraar

Verplichte risicoanalyse	De AVG verwacht van organisaties dat zij bewust omgaan met privacy, bij nieuwe ontwikkelingen (privacy by design). Maar daarnaast moeten organisaties ook de **risico's** in kaart brengen van de **huidige situatie.**	N	Pas de regels toe op huidige situatie en bepaal met behulp van een risico analyse de gewenste maatregelen om de risico's te verlagen. *(Bij nieuwe verwerkingen/ ontwikkelingen moet vooraf onderzocht worden wat de consequenties zijn voor de privacy, zie privacy by design)*	☐ Risico analyse (Breng de risico's in beeld van de huidige situatie en plan acties in)	Realiseren/classificeren en risicoanalyse Classificeren en risicoanalyse
				☐ Gegevensbescherming-effectbeoordeling : vóóraf bij nieuwe ontwikkelingen	Op dit moment wordt er gewerkt aan een format. voor een gegevensbeschermingseffectbeoordeling.
Documentatie-bewijsplicht	Na 25 mei 2018 hoeven scholen geen melding meer te doen bij de Autoriteit Persoonsgegevens als zij gegevens verwerken, die niet onder het vrijstellingsbesluit vallen.	N	Vrijstelling besluit onder de Wbp vervalt. Een organisatie moet met documenten aan kunnen tonen dat de juiste organisatorische en technische maatregelen zijn	**De instelling moet kunnen aantonen :** ☐ Welke gegevens voor welk doel worden gebruikt en met wie deze gedeeld worden enz. (dataregister)	Landelijk wordt er gewerkt aan een dataregister, dat het organisaties eenvoudiger moet maken om aan deze verplichting te voldoen
	In plaats daarvan krijgen zij een documentatieplicht (bewijsplicht). Alle verwerkingen moeten gedocumenteerd worden op basis van artikel 30 van de AVG.		genomen om aan de AVG te voldoen. Deze gegevens zijn ook nodig als betrokkenen van hun rechten gebruik willen maken.	☐Welke verwerkers-overeenkomsten er afgesloten zijn.	Realiseren/ aan de slag/ afspraken met leveranciers
				☐ Welke toestemmingen er gegeven zijn; bv van foto's	Realiseren/ aan de slag/ Gebruik beeldmateriaal leerlingen
Bewustzijn creëren	Het zorgen voor bewustwording van privacy bij alle betrokkenen.	N	Informatiebescherming en privacy onder de aandacht brengen bij medewerkers, leerlingen en ouders.	☐ Organiseer bewustwordingssessies (voorlichtingsbijeenkomsten) over IBP voor leerlingen en	Communiceren/dialoog met de medewerker/ Training IBP voor medewerkers ***NB:** Er wordt gewerkt aan een*

en				medewerkers, maar ook voor ouders	*'lesprogramma' voor leerlingen*
				☐ Breng informatie beveiliging en privacy regelmatig aan de orde. Bijvoorbeeld bij functioneringsgesprekken en lessen mediawijsheid	
Informatieplicht	Informatieplicht, waarbij alle betrokkenen in begrijpelijke taal op de hoogte gebracht moeten worden van hun rechten en plichten		Duidelijk communiceren met medewerkers, leerlingen en ouders over hun rechten, plichten en wat de organisatie doet om privacy risico's te beperken. (zie ook transparantie)	☐ Publiceer de privacy bijsluiters van de verwerkersovereenkomsten	Zie verwerkersovereenkomsten
				☐ Stel een privacy reglement op in heldere begrijpelijke taal	Realiseren/ aan de slag/ privacyreglement *(**NB**. Er wordt gewerkt aan een nieuwe versie)*
				☐ Communiceer met medewerkers, leerlingen en ouders. Communiceer in begrijpelijke taal	Communiceren Communiceren/dialoog ouder: *Voorbeeldteksten communicatie privacy * afspraken fotograferen en filmen door ouders * privacy bijsluiter
				☐ Communiceer over cameratoezicht	Realiseren/aan de slag/ cameratoezicht

Digitale diensten gebruiken onder de 16	In de AVG zijn voor digitale diensten als sociale media en apps aparte regels opgenomen over die toestemming. Wil je als school dat leerlingen *tijdens de les* sociale media gebruiken? Dus zet je sociale media in als *digitaal leermiddel*? Houd er dan rekening mee dat leerlingen jonger dan 16 jaar daar de *uitdrukkelijke toestemming* voor moeten krijgen van hun ouders/verzorgers.	N	Het is van belang **vooraf** een goede overweging te maken om sociale media in te zetten in de lessen. En na te denken wat te doen als er geen toestemming gegevens wordt. **Let op:** *Het gebruik van Digitaal leermateriaal van de diverse uitgevers vallen hierbuiten. Dit komt bij de bewerkersovereenkomsten terug.*	☐ Leg vast en leg uit wat de overweging is om sociale media in te zetten tijdens de les als digitaal leermiddel. Leg vast wat er moet gebeuren als er geen toestemming gegeven wordt.	
				☐ Ouders/ verzorgers toestemming vragen gebruik sociale media	Er komt een voorbeeld toestemmingsformulier
Verwerkersover-eenkomsten	De AVG legt rechtstreekse verplichtingen op aan de verwerker, hiermee krijgt de verwerker meer risico op aansprakelijkheid.		Voor het po en vo is een convenant Digitale Onderwijsmiddelen en Privacy 2.0 opgesteld. Het belangrijkste punt in het	☐ Verwerkersovereenkomsten regelen met alle partijen, die in opdracht van de school persoonsgegevens verwerken.	Realiseren/ aan de slag/ afspraken met leveranciers/model verwerkersovereenkomst 2.0
	De bestuurder is verantwoordelijk voor de keuze van een specifieke		convenant is de rolverdeling: Scholen hebben **de regie** op wat er gebeurt met de	☐ Checken afspraken leveranciers	Realiseren/ aan de slag/ afspraken met leveranciers/ aandachtspunten afspraken leveranciers

	bewerker en de daarmee gemaakte afspraken; Hij houdt de regie. **Let op:** **•De 'verantwoordelijke' in de Wbp wordt onder de AVG 'verwerkersverantwoordelijke' genoemd** **•De 'bewerker' in de Wbp wordt onder de AVG 'verwerker' genoemd.**		persoonsgegevens. Dit mag niet aan een leverancier (een verwerker) overgelaten worden. De school beslist wat de leverancier wél en niet met de gegevens mag doen. **Het schoolbestuur is eindverantwoordelijk!** Bij het convenant hoort een model verwerkersovereenkomst waarmee je als schoolbestuur de juiste afspraken maakt met leveranciers.	☐ Privacybijsluiter toegankelijk maken voor ouders	Communiceren/dialoog met ouders
Meldplicht datalekken	Onder de AVG is de drempel om een datalek te melden lager dan onder de huidige Wbp : • Elk datalek moet gemeld worden, tenzij er geen risico is voor de vrijheden en rechten van de individuen (de privacy geen gevaar loopt). • Organisaties zijn verplicht alle beveiligingsincidenten en datalekken te registreren.	**U**	Weet wanneer een gebeurtenis een datalek is en geen beveiligingsincident. Zorg er als instelling voor dat er een protocol is rondom datalekken en de afhandeling ervan	☐ Protocol beveiligings-incidenten en datalekken	Realiseren/aan de slag/procedure melden beveiligingsincidenten
				☐ Incidenten registratie regelen	Realiseren/aan de slag/procedure melden beveiligingsincidenten Incidenten registratie
Functionaris voor Gegevensbescher ming	Organisaties 'die persoonsgegevens gebruiken van personen waarop regelmatig en stelselmatig toezicht moet worden gehouden' moeten een Functionaris voor	**N**	Scholen volgen leerlingen, monitoren hun gedrag en vorderingen de hele schooldag, en alle vorderingen worden vastgelegd. Dat wordt ook	☐ Aanstellen FG	*Op dit moment wordt er gewerkt aan een advies richting scholen hoe zij om moeten gaan met de aanstelling van een FG*

	Gegevensbescherming (FG) aanstellen.		regelmatig gerapporteerd aan de ouders (in de rapporten). Dit gebeurt stelselmatig. Zonder dit monitoren en stelselmatig volgen en observeren is onderwijs geven niet mogelijk. De conclusie is dan ook dat een FG verplicht is voor onderwijsinstellingen. Uit eerdere gesprekken met het ministerie van OCW blijkt dat deze visie wordt onderschreven.		Zie voor informatie de site van de Autoriteit Persoonsgegevens..
Technische en organisatorische maatregelen	Persoonsgegevens moeten beveiligd worden volgens de geldende beveiligingsnormen. Dit houdt in dat organisaties moderne techniek moeten gebruiken om persoonsgegevens te beschermen. Daarnaast moet niet alleen naar de techniek gekeken worden, maar ook naar hoe de organisatie met persoonsgegevens omgaat. Passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen	U	Organisaties moeten vooraf nadenken over beveiliging van persoonsgegevens, als zij die willen verzamelen. Onder de AVG is een gegevensbeschermingseffectbeoordeling verplicht (nieuw). Maatregelen moeten worden getroffen worden om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn (dataintegriteit).	☐ Gegevensbeschermingseffect-beoordeling uitvoeren: vóóraf bij nieuwe ontwikkelingen	*Op dit moment wordt er gewerkt aan een format. voor een gegevensbeschermingseffectbeoordeling.*
				☐ Procedure opstellen voor inzage, correctie, verwijdering/ afscherming door betrokkenen	
				☐ Toegangsmatrix opstellen	Hieraan wordt gewerkt en komt in de aanpak onder Realiseren/goed op weg/ Wie mogen gegevens inzien?

	dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd. Passend gegevensbeschermingsbeleid invoeren dat door de verwerkingsverantwoordelijke wordt uitgevoerd.		Maak inzichtelijk wie toegang tot welke gegevens heeft. Informatiebeveiliging en privacy beleid	☐Opstellen Informatiebeveiliging en privacy beleid	Aanpak IBP onder Organiseren

Tot slot…

Naast de voornoemde aandachtspunten moet de onderwijsinstelling stelselmatig en gestructureerd omgaan met privacy binnen de eigen organisatie. Ook de eis om technische en organisatorische beveiligingsmaatregelen te nemen, brengt meer met zich mee dan in voornoemd overzicht is opgenomen. Zoals eerder aangegeven is het afvinken van de aandachtspunten niet voldoende om te voldoen aan privacywet- en regelgeving. Voldoen aan de AVG is een continue proces waar je als school aan moet blijven werken.

De aanpak IBP geeft het po en vo de basis om IBP goed te regelen. Voor instellingen in het mbo is een framework met normen- en toetsingskaders ontwikkeld dat te vinden is bij saMBO-ICT: https://www.sambo-ict.nl/netwerken/informatiebeveiliging/#producten

Colofon

Versie: 0.99 (20 juni 2017)

Auteurs: Kennisnet (Elly Dingemanse, Job Vos)