

De 10 meest gestelde vragen

1. Wanneer moet IBP bij mij geregeld zijn?

Antwoord

De meldplicht datalekken is van kracht sinds 1 januari 2016.

Op 25 mei 2016 is de Algemene Verordening Gegevensbescherming (AGV) in werking getreden, deze bevat een overgangstermijn van 2 jaar zodat de AVG 25 mei 2018 van kracht wordt. Deze overgangsperiode is ingebouwd om organisaties de tijd te geven om alles op orde te krijgen. Door de invoer van de AVG worden o.a. de eisen op het gebied van privacy, de verwerking van persoonsgegevens en de beveiliging daarvan strenger.

Het is dan ook aan te raden uiterlijk 25 mei 2018 jouw IBP op orde te hebben. Maar uiteraard geldt in deze: hoe eerder het IBP beleid geregeld is, hoe beter.

2. Kunnen jullie ons bestuur begeleiden om IBP in te zetten op onze scholen?

Antwoord

Kennisnet en de raden detacheren geen experts om scholen te begeleiden naar een goed IBP beleid. Kennisnet wordt gefinancierd door het ministerie van OCW, en kan vanwege deze subsidie geen activiteiten kan verrichten die 'marktverstoring' zijn: we kunnen geen diensten verlenen of adviezen geven waarvoor scholen zelf juristen, advocaten of ict-adviseurs kunnen inschakelen. Kennisnet is geen advieskantoor.

Dat laat onverlet dat we scholen (en het onderwijsveld als geheel) wel kunnen helpen om IBP op orde te krijgen. Om dit uitgebreide onderwerp hanteerbaar te maken, hebben we een 'kapstok' ontwikkeld. Deze pragmatische 'Aanpak IBP' helpt scholen om een (kort) beleid te maken, en op basis daarvan de nodige activiteiten te starten en afspraken vast te leggen. De aanpak bevat uitleg, voorbeelden en templates.

De aanpak bestaat uit drie grote stappen en bevat uitleg, voorbeelden en templates:

- Organiseren (schrijven van beleid)
- Realiseren (activiteiten, documenten, afspraken met leveranciers)
- Communiceren (awareness en voorlichting voor leerlingen, docenten en ouders)

Onze ervaring leert dat veel vragen van scholen beantwoord worden in deze 'Aanpak IBP'. We willen jou dan ook uitnodigen om deze aanpak door te nemen en te kijken of je het antwoord op jouw vraag (vragen) daarin kan terugvinden.

Mocht je nog vragen hebben over dit onderwerp: vragen van scholen over informatiebeveiliging en privacy helpen ons wel. Daardoor weten we wat er leeft binnen scholen. En als een vraag vaak terugkomt, dan kunnen we besluiten om daar bijvoorbeeld een artikel op onze website aan te wijden of om de aanpak uit te breiden. Daarmee helpen we ook andere scholen met jouw vraag!

3. Moet ik met alle leveranciers een bewerkersovereenkomst afsluiten?

En hoe zit het met netwerkbeheerders?

Antwoord

Met iedere leverancier zal het schoolbestuur (voor alle scholen die onder dat bestuur vallen) een bewerkersovereenkomst moeten afsluiten. De wetgever gaat er van uit dat iedere verantwoordelijke (lees: schoolbestuur) zelf daarbij bepaalt welke leerling gegevens met een leverancier worden gedeeld. Het is dus (helaas) niet mogelijk dat de PO-Raad of VO-raad met alle leveranciers een bewerkersovereenkomst afsluit.

Om partijen te helpen de juiste afspraken te maken over privacy, is er een privacyconvenant afgesloten. Partijen die daarbij zijn aangesloten gebruiken een model bewerkersovereenkomst. Daarmee wordt het afsluiten van een bewerkersovereenkomst met alle leverancier eerder een invuloefening. Juist omdat

alle bewerkersovereenkomsten volgens dezelfde structuur zijn opgebouwd, is het eenvoudiger voor een schoolbestuur om te controleren of de juiste afspraken zijn gemaakt. Een schoolbestuur zal altijd zelf moeten controleren of de bewerkersovereenkomst de juiste onderdelen en elementen bevat en goed is ingevuld door de leverancier.

Voor netwerkbeheerders en software zoals van Microsoft, Google en Apple, zijn er nog geen sector brede afspraken. Wel hebben de PO-Raad en VO-raad getoetst of de voorwaarden van deze partijen overeenkomsten met de uitgangspunten van het privacyconvenant. Voor [Microsoft](#) is inmiddels duidelijk dat dat het geval is. Voor Google en Apple wordt de uitkomst van die vergelijking verwacht in de loop van 2017.

Voor netwerkbeheerders zoals Heutink ICT kan er gebruik worden gemaakt van de model bewerkersovereenkomst. Dit vraagt wel aanpassing van een aantal voorwaarden. Daarbij is de gedachte dat de leverancier gevraagd kan worden om een bewerkersovereenkomst die het model als uitgangspunt aanhoudt. Er wordt nog onderzocht of deze partijen ook onder het privacyconvenant kunnen gaan vallen.

4. In welke gevallen mag je als school communiceren met bijzondere persoonsgegevens, zoals het BSN van leerlingen?

Antwoord

Alleen in specifieke gevallen mogen bijzondere persoonsgegevens zoals het BSN gedeeld worden met derden. Specifiek voor uitwisseling van informatie met diverse externe partijen hebben wij in de 'Aanpak IBP' informatiebeveiliging en privacy) een speciale pagina gemaakt:

http://maken.wikiwijs.nl/81891/Informatiebeveiliging_Privacy#!page-2484566

Concrete geschreven informatie over bewaartermijnen van persoonsgegevens (en in het bijzonder BSN) kun je hier vinden: <https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/vraag-en-antwoord/welke-organisatiesmogen-mijn-burgerservicenummer-bsn-gebruiken>

<https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/bewaren-vanpersoonsgegevens>

Niet iedere instantie mag het BSN ontvangen, de voornaamste spelregel is dat BSN alleen gebruikt kan worden als alle partijen daadwerkelijk het BSN mogen verwerken.

GGD: in beginsel mogen scholen persoonsgegevens verstrekken aan de GGD, tenzij zou blijken dat er andere manieren zijn om deze gegevens te verkrijgen die minder inbreuk maken op de privacy van de leerling. Er is geen wettelijke plicht voor de school om de opgevraagde gegevens te verstrekken, behalve als er sprake is van een “algemene zorgplicht om een gezonde leeromgeving te waarborgen” (en daarvoor zou de GGD de aangewezen instantie zijn).

Gemeente/ Leerplichtambtenaren: het doorgeven van BSN nummers bij de gemeente is afhankelijk voor welke doelen deze opgevraagd worden. Zo hebben leerplichtambtenaren bijvoorbeeld een wettelijk recht op informatie. Daarbij gaat het vooral om verzuim. Belangrijk uitgangspunt bij het delen van informatie is of de wet iets regelt (ja, de Leerplichtwet), en dataminimalisatie.

Een leerplichtambtenaar heeft alleen recht op die informatie die hij/zij strikt noodzakelijk nodig heeft voor de uitoefening van zijn werk. Het geven van een account (toegang tot de gehele administratie) komt daar niet mee overeen en is zelfs in strijd met de wet. Een leerplichtambtenaar hoeft niet te zien dat een voorbeeldige leerling één uur mist... Het is nog altijd de school die bepaalt welke leerlingen met de leerplichtambtenaar besproken moeten worden.

5. Wat is de wettelijke bewaartermijn voor leerlinggegevens?

Antwoord

In principe geldt voor leerlinggegevens een standaard bewaartermijn van 2 jaar nadat de leerling de school verlaten heeft. Er zijn op deze regel echter een aantal uitzonderingen. We gaan dit jaar aan de

slag om te zorgen dat alle wettelijke bewaartermijnen inzichtelijk worden. De VO-raad geeft dit jaar prioriteit aan het maken van een handleiding voor bewaartermijnen. We zullen deze bekend maken via de Aanpak IBP.

Verder staan op de website van de Autoriteit Persoonsgegevens al wat richtlijnen met betrekking tot de bewaartermijnen van persoonsgegevens:

<https://autoriteitpersoonsgegevens.nl/nl/overprivacy/persoonsgegevens/bewaren-van-persoonsgegevens>

6. Foto's van leerlingen, waar moet ik rekening mee houden?

En hoe kan ik op mijn school het beste omgaan met social media onderwerpen als beeldpesten en sexting?

Antwoord

Het is van belang om van te voren na te denken over de regelgeving rondom foto en videomateriaal en dit in het beleid op te nemen. Zo is het voor medewerkers, leerlingen en ouders duidelijk wat wel en wat niet toegestaan is. Meer informatie over hoe je dit binnen jouw school kan oppakken en hoe je een gesprek hierover met ouder kan vormgeven, vind je terug in de 'Aanpak IBP': en in dit artikel van de AVG: <https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europeseprivacywetgeving/algemene-verordening-gegevensbescherming#mag-ik-als-school-onder-de-avg-nog-foto's-vanleerlingen-op-internet-publiceren-5994>

Ter ondersteuning van een goed beleid voor de omgang en gedragscodes met betrekking tot social media is deze [leidraad](#) ontwikkeld. Hierin wordt omschreven met welke situaties rekening gehouden moet worden (sexting, beeldpesten etc.) en hoe dit vormgegeven kan worden.

7. Mogen we camera's ophangen op school om pesten te voorkomen?

Een school wil bewakingsbeelden gebruiken om mogelijk pestgedrag vast te leggen. Deze camera wordt opgehangen in de gang van de school. Op deze gang komen de klaslokalen uit van de diverse groepen. Onze vraag is of dit wel kan in verband met de privacywetgeving? Mag je deze beelden ook gebruiken om de pester te confronteren met zijn pestgedrag?

Antwoord

Belangrijk in deze kwestie is het dat de school eerst moet nagaan of er geen andere mogelijkheid is, die minder ingrijpend is voor de privacy van betrokkenen. Vervolgens kan dan op grondslag van het gerechtvaardigd belang besloten worden dat camerabeelden noodzakelijk zijn om de sociale en fysieke veiligheid van leerlingen te garanderen. In dit kader mag de pester met dit gedrag geconfronteerd worden.

Vervolgens moet er wel rekening gehouden worden met de informatieplicht (naar ouders en leerlingen), bijvoorbeeld via website, welke mogelijk gelijk al een preventieve rol kan hebben. Ook moet het bewaartermijn van 4 weken in beschouwing genomen worden. Wanneer er een incident plaatsvindt, wordt deze bewaartermijn verlengd (tot de afhandeling van het incident). Verder moet bewust worden omgegaan met het schriftelijk vastleggen van de kwalificatie van het gedrag. Denk bijvoorbeeld aan vragen als; 'Waar wordt het pestgedrag genoteerd?', 'Wie kan dit inzien?' en 'Welke namen worden hier genoemd?'.

Voor meer informatie over dit onderwerp wil ik je graag doorverwijzen naar cameratoezicht in de Aanpak onder het kopje samen vooruit.

8. Hoe kan ik het beste privacygevoelige gegevens (persoonsgegevens) delen met anderen?

Is een SharePoint omgeving veilig? Kan ik persoonsgegevens versturen via de e-mail? Of zijn er nog andere mogelijke systemen op de markt die betaalbaar en betrouwbaar zijn voor het onderwijs?

Antwoord

E-mailen van persoonsgegevens kan niet zonder meer. E-mail kent zelf geen standaard beveiliging. Mogelijkheden om alsnog via e-mail te versturen zijn versleuteling van de bestanden (en het wachtwoord verstrekken via een ander kanaal) of gebruik maken van mailencryptie. Beide vragen van gebruikers extra handelingen en verdienen niet de schoonheidsprijs. Immers, een gebruiker kan het een keer vergeten en zou zelf terughoudend moeten zijn in het op die manier sturen van persoonsgegevens. Een betere manier is het verstrekken middels een systeem wat aan bepaalde beveiligingseisen voldoet (zodat toegang en verspreiding van persoonsgegevens zo veel mogelijk beperkt worden), waaronder:

- een gebruiker moet inloggen
- je kan aangegeven wie bij bepaalde bestanden/gegevens mag en rechten kunnen intrekken - de beveiliging is op orde
- je weet waar de data staat (en het is niet Amerika)

Dus ja, er zijn andere systemen, maar je moet er zelf de juiste eisen aan verbinden. Op basis van bovenstaande eisen mag Dropbox niet (data in Amerika, en dat mag niet volgens EU-regels omdat daar de privacy minder bescherming kent) en mag SharePoint alleen met een lokale installatie/wanneer je weet dat de data in de EU staat (dus daar moet je opletten bij de voorwaarden en installatie).

9. Ik denk dat er bij mijn school sprake is van een datalek; wat moet ik doen?

Antwoord

Op de website van de Autoriteit Persoonsgegevens kan je meer informatie vinden over hoe je dient om te gaan met een datalek. De Autoriteit Persoonsgegevens heeft een aantal stroomschema's toegelicht om je te helpen:

http://maken.wikiwijs.nl/bestanden/617325/Autoriteit_Persoonsgegevens_Meldplicht%20datalekken%20in%20het%20onderwijs.pdf

In de Aanpak IBP vind je meer informatie over hoe scholen informatiebeveiliging en privacy op school kunnen regelen, datalekken (waaronder een protocol beveiligingsincidenten en datalekken) zijn meegenomen in deze aanpak:

https://maken.wikiwijs.nl/81891/Informatiebeveiliging_Privacy#!page2201229

10. Is het verplicht voor het primair onderwijs (bestuur met meer dan 250 werknemers) een functionaris voor gegevensbescherming (FG) aan te stellen?

Antwoord

Op dit moment is volgens de Wet bescherming persoonsgegevens een functionaris voor gegevensbescherming (FG) nog niet verplicht. Met de inwerkingtreding van de AVG op 25 mei 2018 moeten instellingen zelf bepalen of zij volgens de AVG verplicht zijn een FG aan te stellen. Het aantal van 250 werknemers is geen criterium (meer) om te bepalen of je een FG nodig hebt, ook niet of je gegevens verwerkt van meer dan 5000 betrokkenen. Dat stond eerder wel in de oude teksten.

Volgens artikel 37 van de AVG moet je een FG aanstellen als:

- a. je een overheidsinstelling bent
- b. je organisatie 'hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen'
- c. je belast bent met verwerking van voornamelijk bijzondere persoonsgegevens (zoals medische gegevens).

Voor scholen gaat het om categorie b. Volgens de Engelse tekst van de AVG gaat het om het 'monitoren'. Scholen volgen leerlingen, monitoren hun gedrag en vorderingen de hele schooldag, en alle vorderingen worden vastgelegd. Dat wordt ook regelmatig gerapporteerd aan de ouders (in de rapporten). Dat 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. Uit eerdere gesprekken met het ministerie van OCW blijkt dat deze visie onderschreven wordt.

De verplichting om een FG te hebben geldt per organisatie: niet iedere school hoeft een FG hebben, maar wel ieder schoolbestuur (bevoegd gezag). Daarnaast is het mogelijk dat schoolbesturen samenwerken en samen 1 FG aanstellen. In het mbo is dat inmiddels praktijk aan het worden: 3 of 4 mbo-instellingen regelen samen 1 FG en ze delen de kosten van die FG. De FG mag een interne medewerker zijn, maar kan ook worden 'ingehuurd'. Belangrijke eis is dat de FG op 'naam' moet worden ingehuurd: je kunt niet zeggen dat je een FG hebt (ingehuurd) bij schoolbestuur X, Y of Z, maar je moet de naam vermelden wie je FG is. Dat maakt het lastig om de sectorraden voor de gehele po- of vo-sector een gezamenlijke FG aan te laten stellen.

In de aanpak IBP staat een uitgebreide handreiking FG:

https://maken.wikiwijs.nl/81891/Aanpak_IBP_voor_het_PO_en_VO#!page-3692858