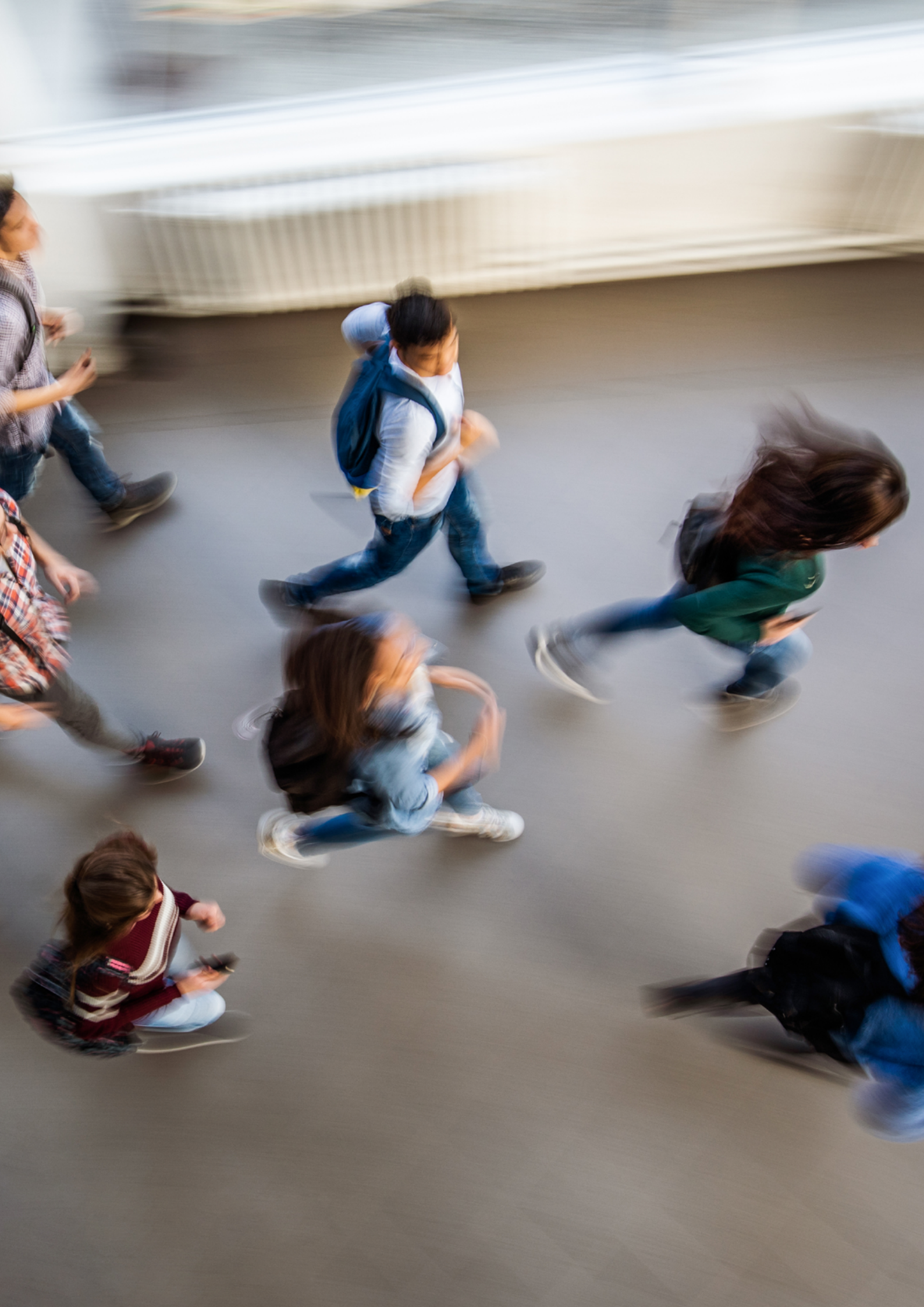
Ingrado

D

De Wpg, wat betekent dat voor domein III onderwijs?



Inleiding

Inleiding

De verwerking van strafrechtelijke gegevens viel tot 25 mei 2018 onder de Wet bescherming persoonsgegevens (Wbp). Door de komst van de Algemene verordening gegevensbescherming (AVG) valt de verwerking van persoonsgegevens rondom strafbare feiten onder een andere Europese wet, namelijk EU-Richtlijn 2016/680. Deze richtlijn is omgezet in de Wet politiegegevens (Wpg), aangevuld met het Besluit politiegegevens BOA (Bpg BOA) en is sinds 1 januari 2019 van kracht.

De opsporing van strafbare feiten valt daarmee buiten het bereik van de AVG. Verwerking van persoonsgegevens op strafrechtelijke grond moet voldoen aan de vereisten van de Wpg. Alle andere verwerkingen – waaronder het toezicht – vallen nog wel onder de AVG. Organisaties hebben daarmee bij de verwerking van persoonsgegevens bij handhavingstaken te maken met zowel de AVG als de Wpg. Dit betekent dat organisaties binnen de bedrijfsvoering rekening moeten houden met voorschriften en verplichtingen uit beide wettelijke regimes.

Hieronder leggen we uit hoe de Wpg van invloed kan zijn op het werk van leerplichtambtenaren en waar je als organisatie aan moet voldoen bij het verwerken van gegevens. We hebben dit gedaan aan de hand van veel gestelde vragen.

De inhoud is tot stand gekomen op basis van vragen die Ingrado heeft ontvangen van haar leden via 'vraag en antwoord' en naar aanleiding van webinars over de Wpg die Ingrado heeft georganiseerd in november 2021.

Deze versie heeft niet de pretentie volledig te zijn. Mocht je aanvullingen, opmerkingen of aanbevelingen hebben, mail deze naar info@ingrado.nl. We zullen de input meenemen in de volgende versie van dit document.

Welke "Wpg" regelgeving is relevant voor de leerplichtambtenaar?

Voor de dagelijkse praktijk van de leerplichtambtenaar is uiteraard de **Wet politiegegevens** relevant. Dat is een zogenaamde raamwet, die in hoofdlijnen een aantal onderwerpen regelt, zoals bijvoorbeeld autorisaties en verstrekkingen. Van belang is te weten dat niet alle bepalingen van de Wet politiegegevens van toepassing zijn verklaard op boa's. In het voor boa's belangrijke Besluit politiegegevens BOA (artikel 2) wordt dit nader geregeld.

In het **Besluit Politiegegevens (BPG)** vind je nadere regels en uitwerkingen voor bijvoorbeeld autorisaties, audits, verstrekkingen aan derden, documentatieplichten en dergelijke.

Voor boa's is het **Besluit politiegegevens buitengewone opsporingsambtenaren** (BPG BOA) van belang. Hierin worden normen, specifiek voor de boa's gegeven. In dit besluit staan onder meer aanvullende verstrekkingsmogelijkheden voor boa's.

Wat zijn politiegegevens?

Politiegegevens zijn persoonsgegevens die in het kader van de politietaak worden verwerkt. Met de politaak moet voor leerplichtambtenaren worden verstaan het doen van een strafrechtelijk onderzoek naar overtredingen uit de Leerplichtwet. Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Een overledene of rechtspersoon valt dus niet onder het begrip persoonsgegeven. Iemands naam, adres en woonplaats zijn voorbeelden van persoonsgegevens. Maar ook telefoonnummers zijn dat.

Wat zegt de Wpg over de kwaliteit van het procesverbaal?

Houd verslaglegging altijd kort, zakelijk en objectief. Leg zoveel mogelijk redenen van wetenschap vast: wie, wanneer, waar, wat, waarom, hoe verkregen en van wie. Zorg dat de gegevens die je verwerkt juist, volledig en actueel zijn. Leg niet meer vast dan noodzakelijk voor het doel van je verwerking. Zorg dat duidelijk uit jouw verslaglegging blijkt of er sprake is van een persoonlijk oordeel of interpretatie of van een feit. Laat indien mogelijk ook collega's tegenlezen. Dat bevordert de kwaliteit. Zo mogelijk zijn systemen voorzien met bijvoorbeeld een koppeling met de basisregistratie personen (BRP) Ook dit voorkomt onjuistheden. Indien blijkt dat een politiegegeven niet juist is, wordt dit weggegooid of gecorrigeerd. (Art 3 en 4 Wpg).

Moet er onderscheid worden gemaakt in categorieën betrokkenen?

Ja, in de informatiesystemen wordt zo mogelijk onderscheid gemaakt tussen verschillende categorieën van betrokkenen (art. 6b Wpg). Het gaat om het onderscheid in verdachten, slachtoffers, veroordeelden en derden. Het gaat er om dat het systeem het mogelijk maakt om de status van de betrokkene aan te geven. Heeft de betreffende persoon de rol van verdachte of die van getuige? In het proces-verbaal wordt dit onderscheid in ieder geval wel gemaakt.

Mag ik bijzondere categorieën van politiegegevens verwerken?

De verwerking van politiegegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, of gegevens over gezondheid, seksueel gedrag en seksuele gerichtheid vindt slechts plaats in aanvulling op de verwerking van andere politiegegevens en wanneer dit strikt noodzakelijk is voor het doel van de verwerking (art 5 Wpg).

Leerplichtambtenaren kunnen deze gegevens verwerken als dat bijvoorbeeld te maken heeft met de reden van de afwezigheid.

Wie mogen er allemaal geautoriseerd worden?

De Wpg verstaat onder autoriseren: Het bewust verlenen van bevoegdheden voor het verrichten van handelingen bij het verwerken van gegevens. Autorisaties worden verleend op basis van het 'Need to Know' principe. Functionarissen krijgen toegang tot de informatie die zij nodig hebben voor het uitoefenen van de functie. In de praktijk betekent dit dat in beginsel alleen boa's toegang krijgen tot de politiegegevens.

Mag je als organisatie ook niet boa's autoriseren?

Ja, dat mag. Artikel 3 BPG BOA biedt voor niet boa's een aantal uitzonderingen. Het moet dan wel noodzakelijk zijn voor de taakuitvoering van de betreffende persoon ('Need to Know' principe). Denk bijvoorbeeld aan de toezichthouder, dus de leerplichtambtenaar die niet beschikt over de BOA bevoegdheid. Denk daarbij ook aan de medewerker die administratieve werkzaamheden met betrekking tot een proces-verbaal (zoals verzenden of voorbereiden van processen-verbaal) verricht of een juridisch medewerker die een inzage verzoek moet afhandelen.

Waar moet je als organisatie aan denken bij het autorisatieproces?

Als organisatie moet je het volgende regelen:

- Een overzicht van wie er allemaal toegang hebben tot politiegegevens
- Een door de verwerkingsverantwoordelijke vastgestelde instructie voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens.
- Het uitvoeren van periodieke controles van de toegekende autorisaties voor alle applicaties.
- De autorisatie moet een duidelijke omschrijving bevatten van de verwerkingen waartoe de boa of niet boa (bijvoorbeeld een toezichthouder) wordt geautoriseerd.
- De toegekende autorisaties moeten in het Wpg register worden vastgelegd. (Wpg, artikel 31, eerste lid j).

Wat houdt de geheimhoudingsplicht voor boa's in?

Boa's zijn op grond van de Wpg verplicht tot geheimhouding. Schending van deze plicht is overigens een strafbaar feit (art. 272 WvSr). De geheimhouding geldt natuurlijk niet als de boa rechtmatig gegevens deelt op grond van de Wet politiegegevens. De geheimhouding geldt ook niet als de boa verplicht wordt gegevens te delen of zijn taak daartoe noodzaakt.

Onder welke grondslag uit de Wpg valt het opmaken van een PV?

De Wpg benoemt voor de BOA een aantal grondslagen voor het verwerken van politiegegevens, namelijk:

- **Dagelijkse politietaak** (art. 8)
- Handhaving rechtsorde in een bepaald geval (art. 9)
- Ondersteuning van de politietaak (art. 13)

Onder de uitvoering van de **dagelijkse politietaak**, vallen het uitvoeren van kleinschalige opsporingsonderzoeken. Ze duren doorgaans korter dan een week en er worden geen bijzondere opsporingsbevoegdheden (BOB) ingezet, zoals het afluisteren van de mobiele telefoon, stelselmatige observaties en dergelijke. Doe je dat wel dan valt het onderzoek onder de doelomschrijving van artikel 9 van de Wpg.

Leerplichtambtenaren gebruiken geen bijzondere opsporingsbevoegdheden en de onderzoeken duren maar kort. Het domein onderwijs valt daarom onder het verwerkingsdoel van **artikel 8 van de Wpg**.

Hoe lang mogen de pv's worden bewaard?

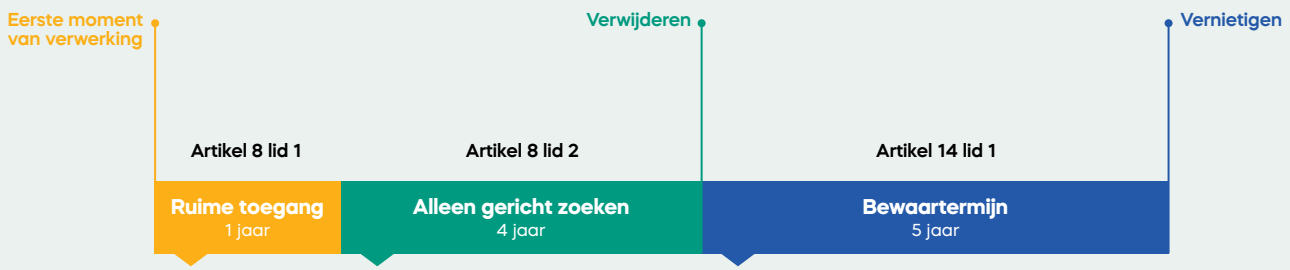
Leerplichtambtenaren verwerken politiegegevens onder de grondslag van artikel 8 Wpg. Voor iedere grondslag kent de Wpg aparte termijnen. De termijnen van artikel 8 zijn dus van toepassing. Van belang is dat je de startdatum van de verzuimmelding vastlegt. Immers vanaf dat moment start het onderzoek naar het strafbare feit en gaat de verwerkingstermijn lopen. Gedurende één jaar mag je dan gegevens die je hebt verkregen om het proces-verbaal op te maken vrijelijk verwerken.

Als de gegevens na een jaar achter het schot zijn gezet (dus beperkt toegankelijk voor medewerkers die daartoe geautoriseerd zijn), blijven de gegevens tot uiterlijk vijf jaar na de startdatum aanwezig, daarna worden ze verwijderd. Dat wil zeggen de gegevens zijn er nog wel maar je mag ze niet meer voor operationele doeleinden inzetten. Alleen voor bijvoorbeeld klachtafhandelingen en audits zijn die gegevens nog benaderbaar. (Dit kun je bijvoorbeeld bereiken door medewerkers te de-autoriseren). Vijf jaar na het verwijdermoment worden deze politiegegevens vernietigd.

Op een plaatje ziet dat er uit zoals hieronder.

Aan te bevelen is om het systeem zodanig in te richten dat deze de termijnbewaking volledig zelfstandig uitvoert. Handmatig mag uiteraard wel maar is zeer bewerkelijk. De bewaartermijnen gelden overigens ook voor fysieke processen-verbaal. Aan te bevelen is verder een functionaris aan te wijzen die toeziet op het naleven van deze termijnen.

Werk altijd in de daarvoor bestemde systemen zoals LBA of Carel en gebruik zo min mogelijk netwerkschijven. Dit helpt je om conform de Wpg te werken en gegevens bijvoorbeeld tijdig te verwijderen.



Mag ik een pv dat ouder is dan een jaar nog wel gebruiken?

Na een jaar zijn de gegevens niet meer vrij toegankelijk. Wel mag je er nog naar zoeken. Je wilt bijvoorbeeld weten of er tegen een leerling al eens eerder proces-verbaal is opgemaakt. Door op naam te zoeken (in opsporingsland noemen ze dit zoeken op “hit no hit basis”) vind je het proces-verbaal dat bijvoorbeeld drie jaar eerder is opgemaakt. Dit zoeken wordt onder de Wpg geautomatiseerd vergelijken genoemd. De gevonden gegevens mag je dan weer gebruiken in het op te maken proces-verbaal.

Zoeken mag alleen gedaan worden indien dat noodzakelijk is voor de uitvoering van de politietaak. Het is dus niet toegestaan om puur uit nieuwsgierigheid of voor privédoeleinden te zoeken.

Met wie mag ik allemaal gegevens uit het pv delen?

Opsporingsambtenaren delen in beginsel met elkaar informatie, als dat nodig is voor hun taken. Dat is het uitgangspunt. Als je informatie deelt met een opsporingsambtenaar (het maakt niet van welke dienst) dan noemt de Wpg dat overigens **ter beschikking stellen**. Dus ook als de leerplichtambtenaar als boa informatie vraagt aan de wijkagent is de wijkagent in beginsel verplicht die te geven. Uiteraard alleen als dat noodzakelijk is voor de taak van de boa! (Art 15 Wpg). Er zijn nog wel een paar uitzonderingen. Zie artikel 2:13 Bpg en artikel 4 Bpg BOA).

Deel je gegevens met niet opsporingsambtenaren dan noemt de wet dat **verstrekken**. Dus met een toezichthouder bijvoorbeeld. De leerplichtambtenaar als boa kan bijvoorbeeld gegevens delen met zijn collega leerplichtambtenaar zonder BOA bevoegdheid op grond van het Bpg BOA (artikel 7 Bpg BOA). Dit moet je dan wel vastleggen. Er zijn vele mogelijke ontvangers van een verstrekking van politiegegevens. Die staan genoemd in de Wpg, het Bpg en het Bpg BOA. In de praktijk wordt er verstrekt aan HALT en de Raad voor de Kinderbescherming. De wijze waarop dit gebeurt, is overigens vormvrij. Het mondeling delen van gegevens (“op de gang”), meekijken over de schouder naar een beeldscherm of document en het instemmend antwoorden op de vraag of bepaalde gegevens correct zijn vallen hieronder; hou daar rekening mee!

Wat moet ik vastleggen als ik gegevens verstrek?

Het delen met opsporingsambtenaren en het Openbaar Ministerie hoef je niet vast te leggen. (Het is overigens wel verstandig om te doen). Verstrek je aan een niet opsporingsinstantie? Dan moet je dat wel vastleggen. Op grond van artikel 32 lid 5 Wpg juncto artikel 6:4 lid 4 Bpg dient te worden vastgelegd:

- De identiteit van de verzoeker
- De datum van de verstrekking
- Een omschrijving van de verstrekte gegevens
- Het doel van de verstrekking

De wijze van verstrekking hoeft overigens niet te worden vastgelegd.

Hiermee wordt controle mogelijk gemaakt of het verstrekken van gegevens overeenkomstig de wettelijke bepalingen heeft plaatsgevonden. Ook kunnen ontvangers van gegevens die achteraf onjuist blijken te zijn worden geïnformeerd.
Voor elke verstrekking – op verzoek of op eigen initiatief – dient de boa te beoordelen welke gegevens verstrekt kunnen worden. Ook beoordeelt de boa of degene aan wie eventueel verstrekt zal worden, bevoegd is tot het ontvangen van gegevens.

Wanneer je informatie deelt dan moet tevens de Officier van Justitie van het betreffende onderzoek zijn instemming verlenen voor het verstrekken. Hij is immers leider van het opsporingsonderzoek.

Ik ontvang een inzage verzoek van een betrokkene. Wat moet ik doen?

Een betrokkene kan op grond van de Wpg kennis nemen welke informatie over hem verwerkt wordt. Tevens kan hij verzoeken indien deze informatie niet juist is, te wijzigen (aanvullen, verwijderen) of zelfs af te schermen.

Dergelijke verzoeken worden behandeld door een medewerker die daarvoor is aangewezen. Dat zal niet de boa zijn maar een juridisch medewerker. De Wpg (par 4) bevat tevens de voorwaarden waaronder dergelijke verzoeken moeten worden behandeld, zoals identificatie van de verzoeker, de weigeringsgronden informatie te verstrekken en de wettelijke termijnen waarbinnen een verzoek moet worden afgehandeld.

Het advies is dan ook om dit verzoek door te zetten aan de betreffende medewerker. Deze handelt het verzoek af. Een dergelijk verzoek kan worden afgewezen als er een opsporingsbelang is. De betreffende medewerker gaat dan bij de betrokken boa na of zich één van de weigeringsgronden ex. art. 27 Wpg voordoet. Daarom dient ook de Officier van Justitie geraadpleegd te worden. Het uiteindelijke besluit is een besluit in de zin van de Algemene wet bestuursrecht. Naast bestaande rechtsmiddelen heeft iedere betrokkene het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens indien deze van mening is dat verwerking van hem betreffende persoonsgegevens niet in overeenstemming is met de Wet politiegegevens.

Tip voor de organisatie

Advies aan de organisatie is om dit werkproces goed in te richten. Het gaat er om dat snel aan een verzoek van een burger kan worden voldaan. Als een betrokkene om inzage verzoekt, moet ook worden verteld aan welke andere partijen de gegevens zijn verstrekt. Verstrekkingen moeten dus ordelijk worden geregistreerd: veilig en afgeschermd voor onbevoegden, maar eenvoudig doorzoekbaar en leverbaar voor inzageverzoeken.

Kent de Wpg ook een verwerkingsregister?

Ja, ook de Wpg schrijft voor dat de verwerkingsverantwoordelijke (voor de boa is dat overigens de werkgever, zie art 1 onder c Bpg BOA) een schriftelijk register bij moet houden met daarin de verwerkingsgrondslag, welke categorieën van betrokkenen en categorieën van gegevens het betreft, de verwijdertermijnen, wie er toegang hebben en welke technische en organisatorische maatregelen, zoals logging, zijn genomen voor de beveiliging van de gegevens. Ook de verwerker moet een (beperkter) register bijhouden.

Kent de Wpg een verplichte logging?

Ja, in tegenstelling tot de AVG wel. Het volgt uit de richtlijn namelijk EU-Richtlijn 2016/680. Het betreffende artikel is echter nog niet geïmplementeerd in de Wpg. De achterliggende gedachte is dat in het strafrecht de gegevens doorgaans gevoelig zijn en dat het grote gevolgen kan hebben als deze gegevens in de verkeerde handen terecht komen. Logging houdt dan ook in dat wordt vastgelegd wie toegang heeft gehad tot bestanden met politiegegevens en dat dit regelmatig wordt gecontroleerd. Zo kan worden nagegaan of iemand toegang heeft gehad tot politiegegevens, terwijl diegene daartoe onbevoegd was.
De verwerkingsverantwoordelijke (werkgever van de boa) (en de verwerker) moeten het verzamelen, wijzigen, raadplegen verstrekken en het vernietigen van politiegegevens vastleggen.

Implementatietermijn

N.B. De richtlijn voorziet in de mogelijkheid voor de lidstaten om, als dit buitengewone inspanningen met zich zou brengen, de geautomatiseerde systemen uiterlijk in 2023 in overeenstemming te brengen met de verplichting tot logging. In uitzonderlijke omstandigheden is verder uitstel mogelijk tot uiterlijk 6 mei 2026.

Moet je toezicht-en opsporingsgegevens apart van elkaar bewaren?

In organisaties waar boa's werkzaam zijn, zijn er nu twee wetten: de AVG en de Wpg. Dat levert twee aparte gegevensverzamelingen op die aan twee aparte werkprocessen gekoppeld zijn: toezicht en opsporing. Het is raadzaam om de opslag van de gegevens in verschillende informatiesystemen te laten plaatsvinden. Als dat niet lukt zul je in ieder geval moeten labelen zodat duidelijk is wat het doel van de verwerking is: opsporing of toezicht. Check of dit mogelijk is in het systeem dat je gebruikt.

Wat zegt de Wpg eigenlijk over beveiliging?

De Wpg kent enkele bepalingen die over de beveiliging van politiegegevens gaan. Zie artikel 4a en artikel 6:1a Bpg). De verwerkingsverantwoordelijke moet vooraf passende technische en organisatorische maatregelen treffen om de nodige waarborgen in de verwerking in te bouwen ter naleving van de Wpg en ter bescherming van de rechten van betrokkenen. Verder moet je niet meer gegevens gaan verzamelen dan noodzakelijk en mogen politiegegevens niet onbeperkt toegankelijk worden gemaakt voor een onbeperkt aantal personen zonder dat dit door een persoon wordt getoetst. Privacy moet maximaal worden gewaarborgd. (**Privacy by design en default**).

Het idee bij privacy by design is om al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen. Privacy by default vereist dat de standaardinstellingen altijd zo privacyvriendelijk mogelijk zijn.

De organisatie zal dus zelf na moeten denken welke maatregelen passend zijn. Screening, afsluitbare kasten, beveiligde mail etc.

Aan te bevelen is om een risicoanalyse uit te voeren om het gewenste beveiligingsniveau vast te stellen. De baseline informatiebeveiliging overheid (BIO) biedt een normenkader waarmee organisaties kunnen aantonen dat zij goed beveiligd zijn.

Ook kan een gegevensbeschermingseffectbeoordeling (GEB) of te wel (privacy impact assessment) daarbij helpen. Dit is een systematisch onderzoek waarbij wordt gekeken welke stromen politiegegevens er allemaal zijn en waarom de verwerking rechtmatig en noodzakelijk is. Daarna beschrijf je de maatregelen die je gaat nemen om de privacy risico's te verkleinen of weg te nemen. Ook beschrijf je de resterende risico's en geef je aan wat je doet als het toch een keer mis zou gaan.

Is er een meldplicht voor datalekken onder de Wpg?

Ja, net als onder de AVG kent ook de Wpg (art 33a Wpg) een meldplicht datalekken. Het is daarom van belang dat er een procedure is die ook bekend is bij de medewerkers.

Er is sprake van een datalek wanneer er een beveiligingsincident heeft plaatsgevonden **waarbij persoonsgegevens verloren zijn gegaan of waarbij redelijkerwijs niet uit te sluiten valt dat persoonsgegevens onrechtmatig zijn of zullen worden verwerkt**. Niet ieder beveiligingsincident is daarom ook een datalek. Wanneer er enkel sprake is van een zwakke plek in de beveiliging van persoonsgegevens, spreekt men van een beveiligingslek en niet van een datalek. De medewerker die het mogelijke datalek ontdekt dient snel en adequaat te handelen door dit te melden aan de daarvoor aangewezen persoon binnen de organisatie. Die kan beoordelen of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit persoonsgegevens (binnen 72 uur). Als er sprake is van een hoog risico moet het zelfs worden gemeld aan de betrokkene.

Enkele tips om datalekken te voorkomen:
- Zit je als boa in een open ruimte, zonder je af als je dat nodig acht.
- Verwijder gegevens vanaf gegevensdragers zoals je smartphone of zakboekje zo snel als dat kan. Denk ook aan foto's. Voorkom dat deze gesynchroniseerd worden met een Apple- of Google-server. Vermijd sowieso het gebruik van privé-telefoons of tablet.
- Gebruik geen WhatsApp of andere commerciële apps voor onderlinge communicatie. Bel je collega op of gebruik beveiligde e-mails vanuit je werk-account
- Mocht het nodig zijn om gegevens tijdelijk buiten de informatiesystemen op te slaan op bijvoorbeeld je laptop of op papier, zorg dan dat deze achter slot en grendel worden opgeborgen en laat deze zeker nooit in de auto liggen.

Wie houdt er toezicht op de naleving van de Wpg?

Extern toezichthouder is de Autoriteit Persoonsgegevens. Deze kan indien organisaties de Wpg niet naleven een last onder bestuursdwang op leggen maar ook een bestuurlijke boete. Zie art 35c Wpg. Daarnaast benoemt de verwerkingsverantwoordelijke een functionaris voor gegevensbescherming (FG) die ondermeer toeziet op de naleving van de Wpg. Verder heeft de FG een adviserende rol. De functionaris voor gegevensbescherming stelt jaarlijks een verslag op van zijn bevindingen. Dit verslag bespreekt de FG met de verwerkingsverantwoordelijke omdat deze eindverantwoordelijk is voor de verwerking van politiegegevens. Daarnaast dient organisatie ieder jaar een interne audit uit te voeren waarin een specifiek onderdeel van de Wpg wordt beoordeeld. (bijvoorbeeld autorisaties) De Wpg bepaalt dat de externe audit 2 jaar na inwerkingtreding voor de eerste keer moet worden uitgevoerd (in 2021 dus)*. De externe audit vindt vervolgens vanaf 2021 elke vier jaar plaats en heeft betrekking op de gehele uitvoering van de Wpg. Deze externe audit dient door een geregistreerde IT-auditor uitgevoerd te worden. Ter voorbereiding op de externe audit is het aan te bevelen een nulmeting of pre-audit uitvoeren. Hierna weet de organisatie waar die staat en welke verbeterslagen er nog gemaakt kunnen worden.

* De auditplicht is met 1 jaar uitgesteld. Organisaties hebben nu tot en met 31 december 2022 de tijd. Meer informatie vind je hier.

Valt de HALT verwijzing onder Wpg?

Ja, immers de gegevens die de leerplichtambtenaar in dat kader verwerkt, hebben betrekking op een door de jongere gepleegd strafbaar feit uit de Leerplichtwet. Zodra het gaat om het onderzoek of de opsporing van strafbare feiten of de tenuitvoerlegging van een straf (ook de HALT afdoening vermeld in artikel 77e Wetboek van Strafrecht) is de AVG niet van toepassing. De AVG gaat niet over opsporing van strafbare feiten en tenuitvoerlegging van straffen, dat staat in artikel 2 van de AVG. De Richtlijn Opsporing en Vervolging (EU) 2016/680 is dus van toepassing. De richtlijn is geïmplementeerd in de Wpg en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Die laatste wet geldt voor het Openbaar Ministerie.

Vanaf welk moment vallen verwerkingen van leerplichtambtenaren onder de Wpg?

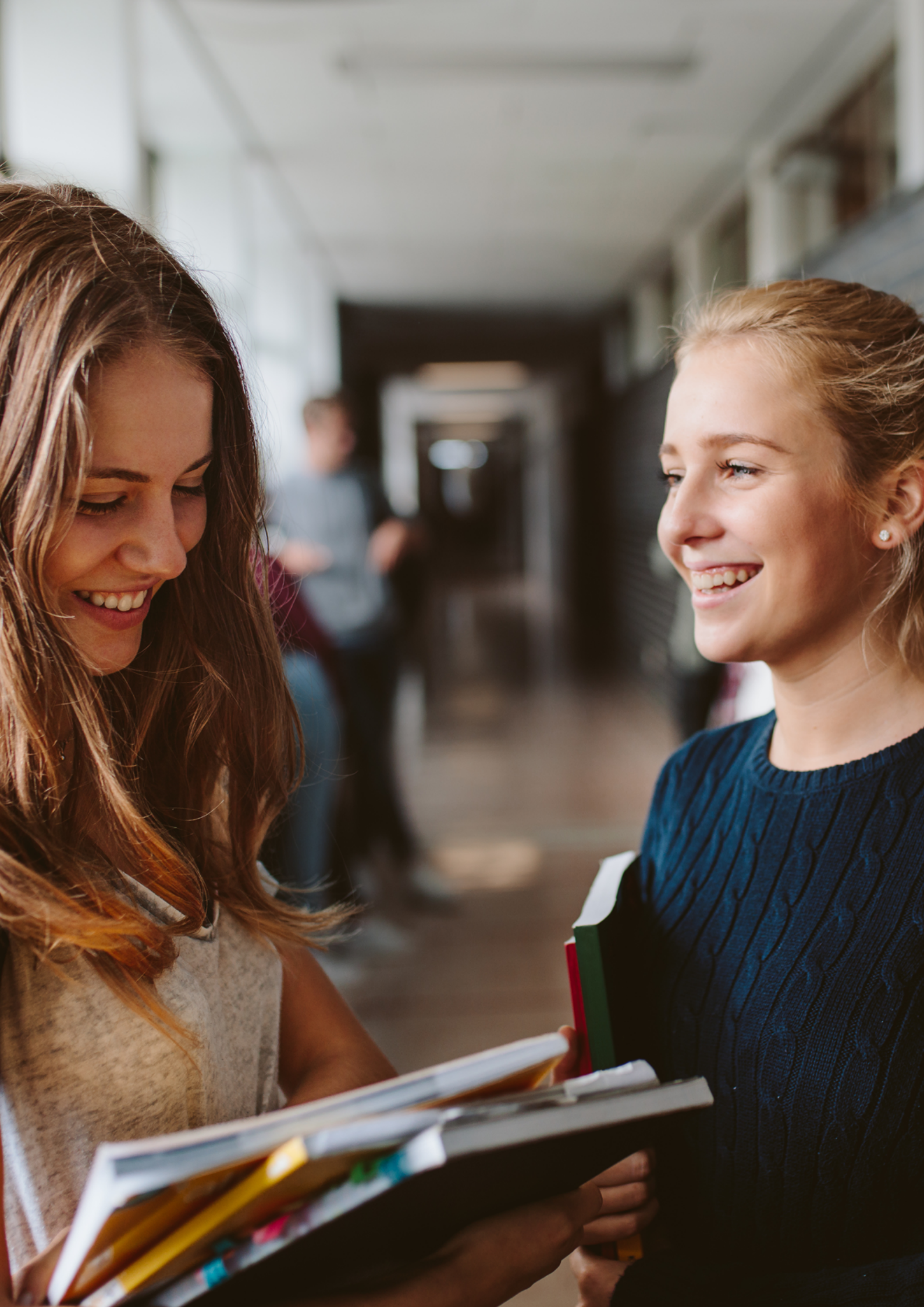
Vanaf het moment dat er een melding gedaan wordt door de school bij de leerplichtambtenaar dat een leerling (vermoedelijk) de Leerplichtwet heeft overtreden. Immers er is dan sprake van een (vermoedelijk) strafbaar feit. Het onderzoek doen naar strafbare feiten en het verwerken van gegevens in dit kader valt niet onder de AVG maar onder de Wpg. Niet alleen het opmaken van een PV valt onder de Wpg maar ook andere activiteiten die je daarvoor hebt vastgelegd in het kader van het strafrechtelijke onderzoek vallen onder de Wpg. Denk daarbij aan notities, gespreksverslagen en dergelijke.

Het behandelen van een beroep op of verzoek tot vrijstelling valt niet onder de Wpg, immers er is dan geen sprake van het doen van onderzoek naar een strafbaar feit. De gegevens die je in dit kader verwerkt vallen onder de AVG.

Kan een leerplichtambtenaar die niet beschikt over de BOA bevoegdheid participeren in een strafrechtelijk onderzoek naar vermoedelijk ongeoorloofd verzuim?

Ja, dit kan op grond van artikel 3 van het Besluit politiegegevens buitengewoon opsporingsambtenaren. De leerplichtambtenaar moet dan wel geautoriseerd worden. De leerplichtambtenaar die geen boa is onthoudt zich daarbij wel van de bevoegdheden waarover alleen de boa op grond van het Wetboek van Strafvordering beschikt. Denk daarbij aan het verhoren van de verdachte en het opmaken van het proces-verbaal.

Deze versie heeft niet de pretentie volledig te zijn. Mocht je aanvullingen, opmerkingen of aanbevelingen hebben, mail deze naar info@ingrado.nl. We zullen de input meenemen in de volgende versie van dit document.



Het recht op onderwijs en ontwikkeling beschermen we samen.

Juist nu!

Ingrado