



Handboek Algemene Verordening Gegevensbescherming (AVG)

Praktische invulling van de AVG voor alle medewerkers binnen Ronduit

1 Inhoud

1	Inhoud.....	2
2	Versiebeheer	3
3	Inleiding.....	4
4	Beeldmateriaal	5
4.1	Regels omtrent schoolfoto's en –video's	5
5	Persoonsgebonden data	6
5.1	Wat zijn persoonsgegevens?	6
5.2	Wat betekent rechtmatig, behoorlijk en transparant?	6
5.3	Bewaartermijnen	7
5.4	Persoonsgegevens delen	8
5.5	Beveiliging	8
5.5.1	Beveiliging persoonsgegevens opgeslagen op papier	8
5.5.2	Beveiliging digitaal opgeslagen persoonsgegevens	8
5.5.3	Overige beveiligingszaken.....	9
6	Datalek	10
7	Samenvatting	10
8	Vragen?	10
9	Belangrijke documenten.....	11

2 Versiebeheer

Versie	Datum	Auteur	Opmerkingen
1.3	23-1-2019	Ronald Oldenhof	Paragraaf delen met derden en bijlagen aangepast
1.2	18-9-2018	Ronald Oldenhof	Paragraaf beeldmateriaal aangepast
1.1	29-5-2018	Ronald Oldenhof	Afbeeldingen en feedback toegevoegd
1.0	24-5-2018	Ronald Oldenhof	1 ^e te publiceren versie
0.1	24-1-2018	Ronald Oldenhof	1 ^e aanzet voor document

3 Inleiding

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze wet, die in geheel Europa geldt, vervangt de Wet Bescherming Persoonsgegevens (WBP) die sinds 2016 in Nederland gehanteerd werd. De AVG zorgt o.a. voor meer verantwoordelijkheden voor organisatie en voor een versterking en uitbreiding van de privacyrechten ten opzichte van de WBP.

Dit handboek geeft praktische invulling van de AVG voor alle medewerkers binnen Ronduit.

Het handboek heeft een dynamisch karakter immers de wetgeving speelt continue in op de technische ontwikkelingen. Maar ook veranderende werkprocessen zijn van invloed op dit handboek. Check regelmatig of je de meest recente versie gebruikt.

Informatiebeveiliging en privacy kun je als schoolbestuurder, schoolleider of ICT-coördinator niet alleen. Je moet het samen doen.

Job Vos, jurist Kennisnet specialisme privacy en informatiebeveiliging in het onderwijs

4 Beeldmateriaal

Het maken van foto's (en eventueel video's) is een veel voorkomende activiteit op scholen. Hoe leuk is het om leerlingen te fotograferen wanneer de leerkracht jarig is of tijdens het bezoek van Sinterklaas. Maar wees je bewust dat het maken van foto's en video's impact heeft op de privacy van degene die op beeld wordt vastgelegd. Het zonder toestemming fotograferen (en filmen) van kinderen is niet toegestaan en kan leiden tot een geldboete met een maximum van 20 miljoen euro. Om een boete te voorkomen zijn een aantal regels opgesteld.

4.1 Regels omtrent schoolfoto's en -video's

1. Vraag jaarlijks toestemming van de ouders voor het maken én plaatsen van foto's en video's. De school kan volstaan met een eenmalig ondertekening van het toestemmingsformulier uit de bijlage op pagina 11. Daarna dient jaarlijks gevraagd te worden of deze toestemming nog van kracht is (zie ook punt 4).
2. Geef aan voor welke media toestemming wordt gegeven. Voor opvallende zaken als een poster of de voorkant van de schoolgids, dient apart toestemming gevraagd te worden.
3. Sla de getekende digitale of gescande toestemmingsbrief op.
4. Zaken goed beveiligd administreren en aantoonbaar jaarlijks bij ouders bevestigd krijgen dat toestemming nog steeds (niet) geldt. Dat hoeft niet met hetzelfde formulier.
5. De school is geen publiek gebouw. Foto's en video's door ouders gemaakt op school vallen onder dezelfde regels als de hierboven genoemde schoolregels. De school communiceert hierover zelf met de ouders.
6. Als een ouder een foto of video toch publiceert en er is aantoonbaar gecommuniceerd door de school dan ligt de verantwoordelijkheid bij de desbetreffende ouder.
7. Foto's en video's gemaakt door ouders tijdens activiteiten buiten school (sportdag, schoolreis, etc.) vallen niet onder de verantwoordelijkheid van school. Maar ouders moeten zich natuurlijk wel aan de wet houden. Als zij foto's maken op een openbare plek, bijvoorbeeld de dierentuin, moeten ze zelf opletten dat ze de privacy van de persoon niet schenden.
8. Ook met toestemming van de ouders voor gebruik van de foto plaatsen scholen geen foto's van leerlingen op Facebook. Immers wanneer ouders zich bedenken en de toestemming intrekken is het (bijna) onmogelijk om de foto van genoemde social media verwijderd te krijgen.



5 Persoonsgebonden data

Volgens de AVG *mogen persoonsgegevens enkel verwerkt worden wanneer zij transparant, behoorlijk en rechtmatig zijn voor de betrokkene.* Maar wat betekent dit nu?

5.1 Wat zijn persoonsgegevens?

Allereerst, wat is een persoonsgegeven. Een persoonsgegeven is elk gegeven dat informatie over iemand geeft ofwel naar deze persoon te herleiden is.

In de wet wordt onderscheid gemaakt in twee types persoonsgegevens.

<i>"Normale" persoonsgegevens:</i>	<i>Bijzondere persoonsgegevens hebben betrekking op:</i>
Naam	Ras of etnische afkomst
Adres	Politieke opvatting(en)
Postcode	Religieuze of levensbeschouwelijke overtuigingen
Telefoonnummer	Lidmaatschap van een vakbond / vakvereniging
IP-adres	Gezondheid
E-mail	Seksueel gedrag of seksuele gerichtheid
	Strafrechtelijk gedrag
	Burgerservicenummer

De wet maakt deze tweedeling om de gevoeligheid van de bijzondere persoonsgegevens te benadrukken. Wees kritisch in het vragen naar deze bijzondere persoonsgegevens.

5.2 Wat betekent rechtmatig, behoorlijk en transparant?

Nu duidelijk is wat persoonsgegevens zijn, kunnen wij kijken naar het criteria wanneer deze verwerkt mogen worden.

- Persoonsgegevens mogen niet ineens voor een ander doel worden gebruikt dan waarvoor ze zijn verzameld
Voorbeeld: zo is het niet toegestaan om het telefoonnummer dat door de ouders bij de inschrijving is opgegeven, op te nemen in een bellijst verspreid onder alle ouders. Het telefoonnummer mag pas gedeeld worden wanneer de eigenaar van dat telefoonnummer (ouder) toestemming voor delen met de andere ouders hiervoor geeft.
- Alleen die persoonsgegevens worden verzameld die nodig zijn voor het leveren van een dienst
Voorbeeld: zo mag op openbare basisscholen niet worden gevraagd naar de religieuze of levensbeschouwelijke overtuiging van de leerling
- Verzamelde gegevens juist zijn en zo nodig worden geactualiseerd
Voorbeeld: in het geval van een scheiding dienen de adresgegevens van beide ouders gecontroleerd en vastgelegd te worden
- Bewaren van de gegevens geschiedt in een vorm die het mogelijk maakt om de betrokkenen niet langer te identificeren dan voor het doel van de verwerking noodzakelijk is
Voorbeeld: het bewaren van leerling gegevens die de school hebben verlaten voor een bepaalde periode



5.3 Bewaartermijnen

Eerder is al aangegeven dat informatie alleen met een bepaald doel mag worden opgeslagen. Vraag blijft dan, hoe lang die informatie mag worden opgeslagen.

Voor gegevens over leerlingen en oud-leerlingen worden de volgende bewaartermijn gehanteerd:

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Het onderwijskundig rapport	maximaal 2 jaar	datum van uitschrijving
Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar	datum van uitschrijving
Gegevens over leerprestaties van de leerling	maximaal 2 jaar	datum van uitschrijving
Verslagen van gesprekken met de ouders	maximaal 2 jaar	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	datum van uitschrijving
Adresgegevens	maximaal 2 jaar	datum van uitschrijving
Gegevens van leerling die naar SO school is doorverwezen	minimaal 3 jaar	datum van uitschrijving
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	maximaal 6 maanden	moment van opname
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school ontvangt	minimaal 7 jaar	na afloop van het schooljaar waarop de bekostiging betrekking heeft
Gegevens over in- en uitschrijving	minimaal 5 jaar	datum van uitschrijving
Gegevens over verzuim en afwezigheid	minimaal 5 jaar	datum van uitschrijving
Gegevens met betrekking tot de vergoeding van de kosten verbonden aan leerlingvervoer	maximaal 2 jaar	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	datum van uitschrijving

- **Het betreft hier niet alleen informatie die digitaal is opgeslagen maar ook om informatie die op de traditionele (papier) wijze is vastgelegd.**

5.4 Persoonsgegevens delen

Hierboven is al aangegeven wat persoonsgegevens zijn en hoe lang deze bewaard mogen worden. Maar met wie of welke instantie mogen persoonsgegevens gedeeld worden?

- Persoonsgegevens dienen van de betrokkene afkomstig te zijn. Wanneer dit niet het geval is, dient de betrokkene hierover binnen redelijke termijn, maar uiterlijk binnen één maand, geïnformeerd
- Persoonsgegevens mogen alleen gedeeld worden op basis van één onderstaande gronden:
 - toestemming van de betrokkene;
 - uitvoeren van een overeenkomst;
 - wettelijke verplichting;
 - vitaal belang van de betrokkene;
 - uitvoeren van een publiekrechtelijke taak;

Voorbeeld: een goed moment is om bij de registratie van een leerling de te informeren over de ontvangers of categorieën van ontvangers.

5.5 Beveiliging

Een belangrijk onderdeel binnen de AVG is de beveiliging van de opgeslagen informatie. In deze paragraaf een beschrijving hoe om te gaan met de opgeslagen informatie. Sommige van deze handreikingen zijn wellicht vanzelfsprekend en worden op de school al gedaan desalniettemin worden ze hier genoemd om de kans op datalekken te verminderen en te voorkomen.

5.5.1 Beveiliging persoonsgegevens opgeslagen op papier

- Zorg ervoor dat documenten met persoonsgegevens, dossiers, etc. zijn opgeslagen in een met een slot gesloten kast
- Documenten met persoonsgegevens liggen niet onbeheerd op een bureau of een tafel
- Ga verantwoord om met documenten met persoonsgegevens:
 - Houd documenten met persoonsgegevens zoveel mogelijk op school.
 - Indien dossiers overgedragen moeten worden, overhandig ze dan persoonlijk of laat ze aangetekend versturen.
- Meld verloren of gestolen documenten met persoonsgegevens volgens de procedure "Melden datalek". Deze is op Sharepoint te vinden. Zie **Belangrijke documenten** op pagina **11**.

5.5.2 Beveiliging digitaal opgeslagen persoonsgegevens

- Sla bestanden met persoonsgegevens op in de Cloud¹. SharePoint en OneDrive zijn de voor de school beschikbare Cloud omgevingen. Het gebruik van USB als opslag van bestanden met persoonsgegevens is onveilig en daarom verboden.

- Documenten met persoonsgegevens worden intern niet als bijlage gemaild maar de link naar het document op SharePoint of OneDrive wordt gedeeld

Voor het delen van dit type document met externen wordt binnen Ronduit gebruik gemaakt van SharePoint. Voor het beveiligd delen met derden is een handleiding beschikbaar. Zie **Belangrijke documenten** op pagina **11**.

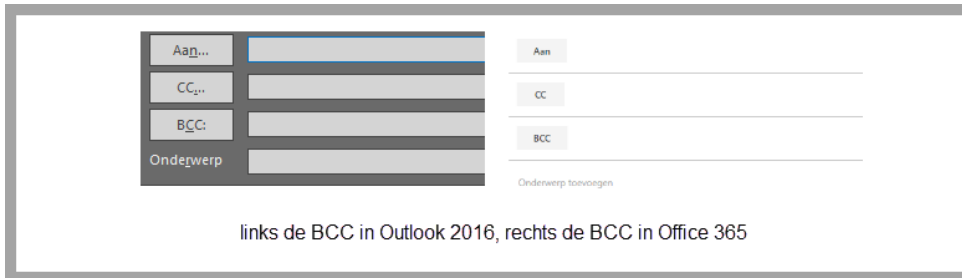


¹ De Cloud staat voor een netwerk dat met al de computers die erop aangesloten zijn een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan. (bron: Wikipedia)


5.5.3 Overige beveiligingszaken

- Wanneer een email naar meerdere mensen wordt gestuurd, maak dan gebruik van BCC. Het inzichtelijk maken van adressen anders dan die eindigend op @ronduitonderwijs.nl is met het van kracht worden van de AVG verboden. Tenzij de ontvanger daar toestemming voor heeft gegeven.

Maar ook wanneer alle geadresseerden een emailadres hebben eindigend op @ronduitonderwijs.nl is het goed om na te denken over het gebruik van een BCC. Een goede manier om erachter te komen of het raadzaam is om BCC te gebruiken is door jezelf af te vragen of alle geadresseerden zitten te wachten op een reactie van één van de geadresseerde wanneer deze bewust of onbewust kiest voor *allen beantwoorden*.



- Wachtwoorden zijn een belangrijk onderdeel in de beveiliging. Hieronder enkele tips voor gebruik van wachtwoord(en).
 - Maak wachtwoorden van minimaal 8 tekens
 - Neem in je wachtwoord een combinatie van cijfers, vreemde tekens (@#\$%&), hoofdletters en kleine letters op
 - Gebruik geen voor de hand liggende informatie in je wachtwoord
 - Gebruik niet één wachtwoord voor meerdere websites of toepassingen
 - Verander regelmatig je wachtwoord(en)
 - Schrijf wachtwoord(en) niet op
 - Communiceer wachtwoord(en) niet met anderen
 - Laat anderen niet meekijken wanneer je je wachtwoord intypt

- Druk gelijktijdig de Windows toets en de letter L ( +L) in om de pc te vergrendelen wanneer je niet achter je pc zit. Dit vormt een extra beveiliging om misbruik van je account voorkomen.



- Met de vele toepassingen in de Cloud is het mogelijk om op andere locaties of met andere apparatuur te werken dan op school. Wees daarom bewust van waar je inlogt. Publieke wifi is niet veilig, het gebruik van publieke wifi om Cloud toepassingen te benaderen wordt om die reden dan ook afgeraden.
- Meld je af (uitloggen) van de Cloud toepassing voordat je de toepassing afsluit. Met het kruisje afsluiten van het venster (rechtsboven) of de pc uitzetten is (vaak) niet voldoende. De volgende persoon die dezelfde computer gebruikt kan op deze manier toegang krijgen tot jouw bestanden/ informatie in de Cloud.
- Binnen Ronduit wordt gebruik gemaakt van beveiligd printen. Iedere medewerker heeft een unieke code ontvangen. Deze code heeft dezelfde normering als een wachtwoord; deel deze code niet met anderen. Voor externen zijn speciale codes aangemaakt.
- Veel mensen gebruiken hun telefoon om ook daar de werkmail op te lezen. De telefoon waarop je dat doet kan een mogelijke oorzaak zijn van een datalek. Zo is het goed om je te realiseren dat bestanden die je downloadt vanuit diezelfde mail onbeveiligd op je telefoon worden opgeslagen. Beter is dan ook om geen bestanden met persoonsgegevens te downloaden. Mochten die toch op je telefoon terecht zijn gekomen, verwijder deze bestanden dan ook direct van je telefoon. Telefoons hebben een optie om op afstand gewist te worden. Zorg dat je dit hebt ingesteld,

zodat je in geval van verlies of diefstal het toestel op afstand kunt wissen waarmee ook de mailbox van je werk wordt verwijderd. Geef verlies of diefstal van je telefoon, uiteraard alleen wanneer daar werkmail op wordt ontvangen, direct door aan je leidinggevende. Deze zal de procedure datalek starten en kan door ICT direct je wachtwoord worden gereset om (verder) misbruik van je account te voorkomen.

6 Datalek

Een datalek ontstaat wanneer iemand toegang heeft tot persoonsgegevens terwijl dat niet mag. Dit kan in digitaal formaat opgeslagen data zijn maar ook wanneer dossiers onbeheerd (op een bureau) zijn blijven liggen.

Het melden van datalekken gebeurt via het formulier dat op de Ronduit SharePoint is te vinden. Op basis van dit ingevulde formulier wordt bepaald of het daadwerkelijk een datalek is en gemeld dient te worden bij de Autoriteit Persoonsgegevens.



7 Samenvatting

Leuk al deze informatie over AVG, maar hoe weet je nu of je volgens de AVG werkt? Om daar antwoord op te geven kun je jezelf de volgende vragen stellen:

1. Leg ik persoonsgegevens vast?
2. Zo ja, heb ik de betrokkene geïnformeerd dat ik die persoonsgegevens heb? M.a.w. heb ik toestemming om deze gegevens in mijn bezit te hebben.
3. Heb ik de betrokkene geïnformeerd over het doel van de persoonsgegevens?
4. Zijn er gronden waarop ik deze informatie mag delen?
5. Zo ja, heb ik de betrokkene geïnformeerd met wie / welke organisaties deze persoonsgegevens gedeeld worden?
6. Heb ik de betrokkene geïnformeerd omtrent de bewaartermijn van deze persoonsgegevens?
7. Heb ik de betrokkene geïnformeerd dat deze het recht heeft om de eerder verleende toestemming in te trekken?
8. Heb ik de betrokkene geïnformeerd dat deze het recht heeft om een klacht bij de Autoriteit Persoonsgegevens in te dienen?

Een belangrijk onderdeel is dus de communicatie met de betrokkene. In het geval van kinderen onder de 16 zijn dat trouwens de ouders.

Wanneer je alle bovenstaande vragen met ja hebt beantwoord, ben je voor de AVG goed op weg!

8 Vragen?

Dit document probeert een antwoord te geven hoe in de praktijk om te gaan met AVG. Het is echter onmogelijk om alle situaties te behandelen. Zit je na het lezen nog met vragen omtrent de AVG in een voor jou specifieke situatie, bespreek dat dan allereerst in je team. Komen jullie er daarna (nog) niet uit dan kun je je vraag per e-mail stellen aan avg@ronduitonderwijs.nl. Beschrijf je vraag en specifieke situatie zo uitgebreid mogelijk.

Hetzelfde e-mailadres kun je ook gebruiken voor verbeterpunten voor dit document.

9 Belangrijke documenten

Handleiding bestanden delen:

https://ronduit.sharepoint.com/ICTgroep/Mijn_ICT_coach/Sharepoint/Delen_met_externen_via_Share-Point.pdf

Link melden datalek:

<https://ronduit.sharepoint.com/MeldenDataLek>

Formulier toestemming foto (alleen beschikbaar voor directies en ICT coördinatoren):

https://ronduit.sharepoint.com/AVG/Sjablonen/Sjabloon_brief_toestemming_gebruik_foto_s_en_video_s_versie_012019.pdf