paraat scholen | altijd in ontwikkeling

- BELEID -

AVG, Algemene Verordening Gegevensbescherming

Inhoudsopgave

1. Verkorte weergave beleid

Het beleid in dit document heeft betrekking op alle onder ons bestuur vallende scholen en het bestuurskantoor. Het betreft:

- 06CP De Wegwijzer
- 06DF Het Hof
- 07FK De Slinger
- 12IL De Drie Linden
- 13JK Op Koers
- 13JK1 De Wegwijzer
- 13ON Leemvoort
- 18FK 't Montferland
- 18FM De Woelwaters
- 03UN Antoniusschool Lievelde
- 05HW Jozefschool
- 06ZO Antoniusschool Vragender
- 07BK Canisiusschool
- 08NH De Regenboog
- 08RR Theresiaschool
- 09MG Frans ten Boschschool
- 10HC Pastoor van Arsschool
- 10XV Jozefschool
- 11LO Jorisschool
- 14VP Ludgerusschool

1.1 Inleiding

Op 25 mei 2018 zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG in werking getreden. Concreet betekent dit dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. Het doel van het aanscherpen van de regels die betrekking hebben op de privacy van mensen, is het waarborgen van de rechten van ieder mens in een complexe (digitale) wereld. De verordening streeft gelijkheid na voor iedereen binnen de Europese Unie.

De AVG zorgt onder meer voor:

- Versterking en uitbreiding van de privacy rechten
- Meer verantwoordelijkheden voor organisaties
- Dezelfde bevoegdheden voor alle Europese privacy toezichthouders (te denken valt onder meer aan het opleggen van boetes bij schending van de privacy)

Voor iedere werkgever geldt, met betrekking tot de privacy van alle werknemers en stakeholders: **100% accountability** d.w.z. een waterdichte verantwoordingsplicht als het gaat om de privacy van de werknemers en andere stakeholders.

Binnen de AVG zijn er drie actoren:
De verwerkersverantwoordelijke: dat is Paraat. De verwerkersverantwoordelijke dient een aantal verplichte maatregelen in te voeren waaronder:

- het bijhouden van een register van verwerkingsactiviteiten
- het bijhouden van een register van datalekken

- het aantonen dat betrokkene aantoonbaar toestemming heeft gegeven voor de verwerking van zijn/haar gegevens
- het aanstellen van een Functionaris gegevens bescherming
- het opstellen van een gedragscode
- het afleggen van verantwoording van alles wat te maken heeft met de AVG, binnen het jaarverslag

De verwerker: degene die gegevens verwerkt
De betrokkene: de persoon met zijn/haar gegevens, de betrokkene heeft binnen de AVG specifieke rechten:

- het recht van inzien
- het recht op bevriezing van verwerking
- het recht om 'vergeten' te worden (het definitief verwijderen van de gegevens)
- het recht om zijn/haar gegevens over te (laten) dragen
- het recht op informatie over zijn/haar gegevens
- het recht op het melden van een data lek
- het recht op verzet op verwerking
- het recht op data portabiliteit

De AVG omvat het totaal van het verwerken van gegevens die herleid kunnen worden naar een persoon. Van het verzamelen van de gegevens tot aan de vernietiging van de gegevens dus het vastleggen, het ordenen, het bewaren, het bijwerken, het wijzigen, het opvragen, het doorzenden, het verspreiden, het beschikbaar stellen aan derden, etc.

Een correcte implementatie van de AVG omvat zowel technische aspecten als het bijbehorend maatschappelijk debat, de cultuur binnen een organisatie. In dit geval het omgaan met de privacy van betrokkenen.
De organisatiegebieden die de AVG 'raken', zijn onder andere:

- **m.b.t. de leerlingen:** digitale methode toepassingen, inlogcodes, wachtwoorden, gegevens in de groepsmappen, toegang binnen ParnasSys.
- **m.b.t. de medewerkers:** inlogcodes en wachtwoorden, (groeps) communicatie met ouders en derden (denk ook aan bijbehorende foto's), mail en mail met bijlagen, leerling dossiers, ParnasSys, (financiële) administratie, schriftelijke- en mondelinge correspondentie
- **m.b.t. derden:** mail en mail met bijlagen, schriftelijke en mondelinge correspondentie, toegang tot leerling- en oudergegevens
- **m.b.t. beleid en organisatie:** imago en pr-activiteiten
- **m.b.t. ruimten en apparaten:** servers, laptops, computers, printers
- **m.b.t. de continuïteit van de Paraatscholen:** websites en applicaties
- **alle toegangscontrole en inlogactiviteiten**
- **toegangsbeveiliging van gebouwen**

1.2 Vuistregels & het wettelijk bepaalde doel voor Paraat scholen

Voor een correcte toepassing van de AVG, gelden vijf 'vuistregels':

1. **Doelbepaling & 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 wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag & rechtmatigheid:** verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: aantoonbare toestemming, (verwerkers) overeenkomst, een wettelijke

verplichting, publiekrechtelijke taak, vitaal belang van de betrokkene, algemeen belang of gerechtvaardigd belang.

3. **Dataminimalisatie:** minimale gegevensverwerking en opslag. Bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt, het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel, conform artikel 6 AVG, te bereiken. Ze staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie:** heb ik de betrokkene (de leerkracht/de ouder) vooraf helder geïnformeerd over het doel van de gegevensverwerking en is uitgelegd welke gegevens worden gebruikt en met wie ze worden gedeeld alsmede over het gevoerde AVG-beleid.
5. **Data integriteit:** kloppen de gegevens nog en zijn ze op de juiste plek voor de juiste mensen beschikbaar. Er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Voor een onderwijsorganisatie, in dit geval voor Paraat scholen, geldt, in relatie tot de AVG, een wettelijk bepaald doel.
Dat wil zeggen dat het totaal aan verwerken van leerling gegevens alleen rechtmatig is in het kader van:

- Het leren aan- of het geven van onderwijs
- Het leren aan- of het begeleiden van kinderen
- Het verstrekken van of het beschikbaar stellen van leermiddelen
- Het delen van informatie over leerlingen
- Het bekend maken van activiteiten binnen de organisatie
- Het berekenen, vastleggen of innen van vergoedingen en (ouder)bijdragen
- Het behandelen van geschillen
- Het doen uitoefenen van een accountantscontrole
- De uitvoering of toepassing van een andere wet

Dat wil zeggen dat het totaal aan verwerken van medewerkersgegevens alleen rechtmatig is in het kader van:

- Het aangaan, uitvoeren en beëindigen van arbeidsovereenkomsten, meer specifiek de beoordeling van de geschiktheid van betrokkene voor een functie die vacant is of kan komen
- Het geven van leiding aan de werkzaamheden van de betrokkene
- De behandeling van personeelszaken
- Het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura aan of ten behoeve van betrokkene
- Het berekenen, vastleggen en betalen van belasting en premies ten behoeve van betrokkene
- Het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband
- De opleiding van betrokkene
- De bedrijf medische zorg voor betrokkene
- Het bedrijfsmaatschappelijk werk
- De verkiezing van leden van de leden van een medezeggenschapsorgaan

De uitvoering van een voor de betrokkene geldende arbeidsvoorwaarden

Indien wij gegevens 'verzamelen' voor een ander doel dan hierboven genoemd, vragen wij toestemming van betrokkene.

2. Ons beleid voor informatiebeveiliging & privacy

Informatie en ICT zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is de privacywetgeving daarop van toepassing.

Onze informatie en ICT worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens, leiden tot inbreuk op het geven van onderwijs en het vertrouwen in onze organisatie.
Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat, een doel stellen en de manier omschrijven waarop we dit doel willen bereiken.

Overal waar in dit beleidsdocument 'Paraat scholen' wordt genoemd, wordt verwezen naar de rechtspersonen van Reflexis en Lima.

2.1 Informatiebeveiliging & privacy

Informatiebeveiliging is een proces ten behoeve van het beschermen van Paraat scholen tegen risico's en bedreigingen met betrekking tot informatie en ICT. Het richt zicht op drie aspecten:

- **de beschikbaarheid van gegevens:** informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig
- **integriteit:** informatie en verwerkingsmethoden bevatten zo min mogelijk fouten
- **vertrouwelijkheid:** informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving (AVG 2018). Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect 'vertrouwelijkheid' is hiervoor van belang. Informatiebeveiliging is daarom integraal onderdeel van privacy. Om privacy goed te regelen is informatiebeveiliging nodig.
Daarom zien we het als één onderwerp: de AVG.

2.2 Doel & reikwijdte

Ons beleid heeft als doel:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering
- Het garanderen van de privacy van leerlingen (en hun ouders/verzorgers) en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken

Dit beleid is een leidraad voor iedereen die betrokken is bij AVG binnen Paraat scholen en is van toepassing op alle medewerkers, tijdelijk personeel en andere personen die binnen onze organisatie een rol spelen.
Het is van toepassing op de hele organisatie, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het informatiebeveiligings- en privacy beleid heeft raakvlakken met andere beleidsgebieden, te weten:

- Algemeen veiligheids- en beveiligingsbeleid: met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en -beveiliging, crisismanagement, huisvesting en ongevallen
- IT-beleid: met als aandachtsgebieden de aanschaf en het beheer van ICT
- Personeels- en organisatiebeleid: met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties
- Administratie

Dit beleid maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

2.3 Uitgangspunten

De belangrijkste beleidsuitgangspunten, in relatie tot de AVG 2018, bij Paraat scholen zijn:

- Informatiebeveiliging en privacy dienen te voldoen aan alle relevante wet- en regelgeving
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij wet- en regelgeving respecteren en daar hun eigen verantwoordelijkheid in nemen
- Paraat scholen is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt
- Paraat scholen maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld, concrete afspraken over informatiebeveiliging en privacy
- IBP is een continu proces, waarbij de afdeling P&O en de Functionaris Gegevensbescherming regelmatig (minimaal jaarlijks) evalueren en analyseren of er aanpassingen gewenst zijn
- Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid

2.4 Wet- & regelgeving

Paraat scholen voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het Primair Onderwijs
- Wet Goed Onderwijs en Goed Bestuur PO/VO
- Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet AVG
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht
- Convenant 'Digitale onderwijsmiddelen en privacy 3.0' en het daarbij behorende model Verwerkersovereenkomst 3.0 zijn leidend bij het maken van afspraken met leveranciers.

2.5 Organisatie

Dit hoofdstuk beschrijft hoe AVG bij Paraat scholen is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- **Richtinggevend** (strategisch)
- **Sturend** (tactisch)
- **Uitvoerend** (operationeel)

Strategisch niveau
Het College van Bestuur is eindverantwoordelijk voor AVG en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De toepassing en werking van het AVG-beleid wordt op basis van regelmatige rapportages (minimaal 1 maal per kwartaal) door hen geëvalueerd.
Het College van Bestuur is verantwoordelijk voor de uitvoer van- en het toezicht op AVG.

Tactisch niveau
Het College van Bestuur geeft terugkoppeling aan de Raad van Toezicht en advies aan de eindverantwoordelijke en stuurt de mensen aan op de uitvoerende laag.
Het College van Bestuur:

- Vertaalt het beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- Bewaakt de uniformiteit binnen Paraat scholen
- Vormt het aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy
- Zorgt voor een adequate afhandeling van incidenten binnen Paraat scholen

De functionaris voor gegevensbescherming (FG) heeft een specifieke taak en houdt binnen Paraat scholen toezicht op de toepassing en naleving van de privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.
De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. FG heeft regelmatig overleg met het College van Bestuur (per kwartaal is er een stafoverleg). De FG is ook contactpersoon voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

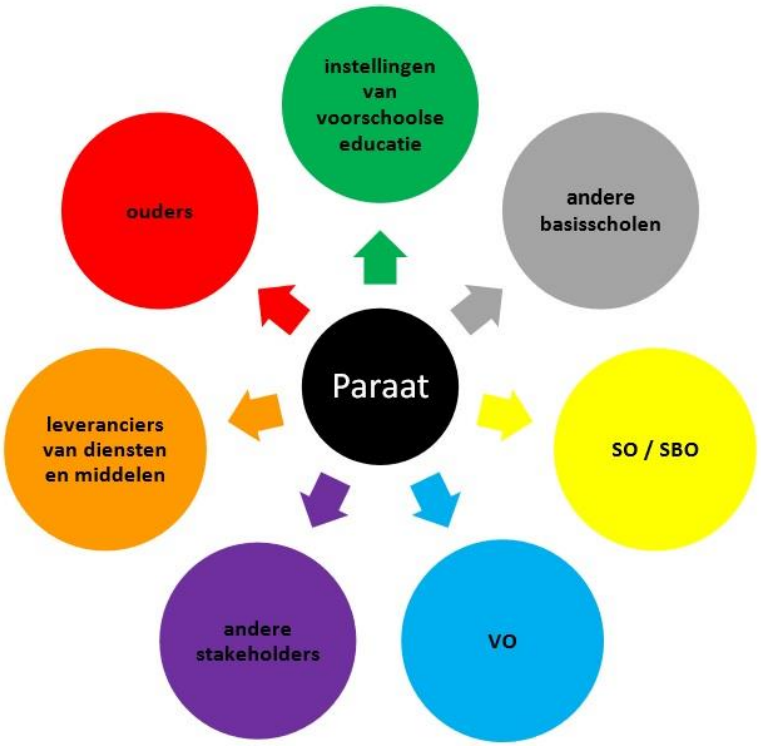
Operationeel niveau
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in dit beleidsstuk. Medewerkers worden onder andere gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering.
Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- Er voor te zorgen dat zijn/haar medewerkers op de hoogte zijn van het beveiligingsbeleid
- Alle medewerkers die met persoonsgegevens werken, hebben geheimhoudingsplicht. Zij zijn hier bij het in dienst treden op gewezen, dan wel hebben een geheimhoudingsovereenkomst ondertekend
- Toe te zien op de naleving van het AVG-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft
- Periodiek het onderwerp AVG onder de aandacht te brengen in werkoverleggen, beoordelingen etc. (De frequentie hiervan zal per school verschillen, dit heeft te maken met de vergaderstructuur op schoolniveau. Minimaal vier maal per jaar is de richtinggevende uitspraak.)
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde AVG-onderwerpen

De leidinggevende kan in zijn taak ondersteund worden door de functionaris voor gegevensbescherming.

2.6 Toetsingskader, statements & beheersmaatregelen

De principes zoals die geldend zijn binnen wet- en regelgeving, zijn vertaald naar concrete toetsbare normen. Deze normen noemen wij 'statements'. Als wij als organisatie aan deze statements voldoen, dan worden de 'bovenliggende' basis-privacy-principes nageleefd (datakwaliteit, doel en ontbinding, de rechten van betrokkene, de grondslag, de beveiliging, dataminimalisatie, bijbehorende verantwoordelijkheden en transparantie). Deze statements hebben betrekking op onze gehele 'organisatie architectuur'.
Onze 'organisatie architectuur' m.b.t. het uitwisselen van gegevens:



Bovenstaande architectuur principes zijn van belang om de risico's op het gebied van privacy te beperken. De top vier van privacy risico's, bij alle bovenstaande stakeholders, zijn:

- Het ontstaan van datalekken
- Ongewenste (interne) publicaties over derden (een medewerker 'deelt' bijvoorbeeld een zorgdossier van een leerling)
- Ongewenste (interne) publicaties over eigen medewerkers (dossiers m.b.t. de gesprekscyclus zijn bijvoorbeeld toegankelijk)
- Een leverancier heeft/gebruikt/hanteert privacygevoelige data op de verkeerde manier

Binnen ons toezichtkader wordt gebruik gemaakt van een 'clustering'. Wij hanteren zes clusters:

1. Beleid & organisatie
2. Personeel, deelnemers & gasten
3. Ruimte & apparatuur
4. Continuïteit
5. Toegangsbeveiliging & integriteit
6. Controle & logging

Het toezichtkader voor onze organisatie behorende bij bovenstaande clusters, wordt in onderstaande paragrafen toegelicht.

2.6.1 Cluster beleid & organisatie

Privacy statements betreffende het cluster 'beleid & organisatie'

1. De beleidsregels ten behoeve van informatiebeveiliging en privacy zijn gedefinieerd en goedgekeurd door CvB en GMR. Dit beleid:
    - Is SMART geformuleerd en omvat ook rollen en verantwoordelijkheden
    - Omvat informatie over **doelbepaling & doelbinding.** Voor iedere categorie van gegevensverwerking is, voorafgaand aan die verwerking, het specifiek doel vastgesteld en naar betrokkenen gecommuniceerd. De gegevens worden alleen gebruikt voor het doeleinde waarvoor die gegevens verkregen zijn.
    - Omvat informatie over **grondslag & rechtmatigheid.** Alle informatie wordt op basis van onze wettelijke grondslag verwerkt. Er wordt gebruik gemaakt 'opt-out regelingen' daar waar het gaat om de verwerking van persoonsgegevens (d.w.z. dat betrokkene aan kan geven dat hij/zij aan een bepaalde regel niet wenst deel te nemen in het kader van de AVG).
      Er is toestemming verleend door de wettelijke vertegenwoordigers van de leerling en deze toestemming is vastgelegd en reproduceerbaar.
    - Omvat informatie over **dataminimalisatie.** Het verwerken van de gegevens moet in verhouding staan tot het doel van de gegevens.
    - Omvat informatie over **transparantie.** Wij kunnen bewijzen dat wij betrokkenen adequaat en eenduidig hebben geïnformeerd.
    - Omvat informatie over **data-integriteit.** Wij zorgen er aantoonbaar voor dat de juiste persoonsgegevens, voor de juiste mensen, op het juiste moment en op de juiste plaats beschikbaar zijn.
2. Het vastgestelde beleid wordt gepubliceerd op de site van Paraat scholen en de scholen en wordt actief gecommuniceerd naar medewerkers en externe partijen.
3. Er is beleid vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich mee brengt, te beheren.
4. Informatiestromen zijn geclassificeerd m.b.t. de wettelijke eisen, waarde, belang en gevoeligheid (risicoanalyse).
5. Relevante informatiebeveiligingseisen zijn vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen.
6. Er is beleid en structuur op gebeurtenissen en incidenten die betrekking hebben op informatiebeveiliging en privacy. Er is een structuur vastgelegd die rapporteren snel en adequaat maakt.
7. Er is een functionaris bescherming persoonsgegevens aangewezen. Zijn/haar taken en verantwoordelijkheden zijn helder geformuleerd en bestaan ten minste uit de volgende taken:
    - Het registreren van verwerkingen van gegevensverwerkingen
    - Het adviseren van de verantwoordelijke en alle bij gegevens betrokken medewerkers over hun (wettelijke) verplichtingen
    - Toezicht op de naleving van wet- en regelgeving, alsmede de naleving van het privacy beleid, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij verwerking betrokken personeel
    - Samenwerking met de toezichthoudende (privacy) autoriteiten
    - Optreden als contactpunt van de toezichthoudende autoriteit
    - Hij/zij houdt een register bij:
        - van de verwerking van alle typen persoonsgegevens
        - van de verwerking van de gegevens van de bewerker van die gegevens
        - van de doeleinden van die gegevensverwerking

        - van een beschrijving van de categorieën persoonsgegevens
        - van een beschrijving van de categorieën betrokkenen (intern en extern)
        - indien er sprake is van het doorgeven van die gegevens buiten de EU
        - van de van toepassing zijnde bewaar- en vernietigingsmaatregelen en de opvolging daar van.
8. Er is een actief archief- en vernietigingsbeleid met bijbehorende bewijslast. Het betreft hier de algemeen geldende termijnen, met het recht van de betrokkene om zijn/haar gegevens te laten vernietigen. Alle medewerkers zijn aantoonbaar geïnformeerd over de bewaartermijn.
9. Er is beleid op de verwerking van bijzondere persoonsgegevens en dit beleid wordt aantoonbaar in de dagelijkse praktijk nageleefd. Wij verwerken geen gegevens betreffende:
    - De religieuze of levensbeschouwelijk overtuiging
    - Ras of etnische afkomst
    - Biometrische gegevens
    - Gezondheid of seksuele voorkeur

    Tenzij dit strikt noodzakelijk is voor de doelen van onze werkzaamheden of wij daartoe op grond van een andere wet verplicht zijn. Hiervoor is expliciet toestemming gevraagd aan betrokkene.
10. Er is een bewerkingsovereenkomst afgesloten met alle leveranciers. Deze overeenkomst omvat in ieder geval de volgende elementen:
    - Het onderwerp waarop de overeenkomst betrekking heeft
    - De duur van de verwerking
    - Aard en doel van de verwerking
    - Het benodigde soort persoonsgegevens
    - De rechten en plichten van de verantwoordelijke en de bewerker
    - De (ondertekende) instructie dat de bewerker alleen na uitdrukkelijke opdracht en instructie, de persoonsgegevens van de stakeholders binnen Paraat scholen zal verwerken
    - Een ondertekende overeenkomst tot geheimhouding
    - De leverancier moet zorgdragen voor adequate beveiliging van de gegevens
    - Contractuele verplichtingen gelden voor alle medewerkers van de leverancier
    - Afspraken omtrent bewaar- en vernietigingstermijnen

2.6.2 Cluster personeel, deelnemers & gasten

Privacy statements betreffende het cluster 'personeel, deelnemers & gasten'

1. De contractuele overeenkomst met medewerkers vermeldt hun verantwoordelijkheden voor informatiebeveiliging.
2. Alle medewerkers en, voor zover relevant contractanten, hebben een passende informatie/training/ scholing verkregen in relatie tot de wet op de privacy en de raakvlakken met hun eigen werkzaamheden.
3. Er is beleid en bewijs dat de toegangsrechten van alle medewerkers worden vernietigd bij beëindiging van het dienstverband of contract.
4. In beleid en de werkzaamheden van de medewerkers P&O is cyclisch vastgelegd dat de eisen voor geheimhoudingsovereenkomsten regelmatig opnieuw worden getoetst, beoordeeld en worden gedocumenteerd.
5. Wij kunnen aantonen op welke wijze wij ouders en medewerkers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en met welk doel informeren over het privacy beleid en de rechten en plichten van alle betrokkenen. Dit betreft ook de bewaar- en vernietigingstermijn en met wie de gegevens gedeeld worden.

2.6.3 Cluster ruimtes & apparatuur

Privacy statements betreffende het cluster 'ruimtes en apparatuur'

1. Er is beleid vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt, te beperken.
2. Alle onderdelen van apparatuur binnen Paraat scholen die opslagmedia bevatten, zijn geverifieerd en gedocumenteerd om te waarborgen dat gevoelige informatie verkeerd wordt gebruikt. Bij de beëindiging van het gebruik van deze apparatuur is er een bewijs van correcte vernietiging van de data en van de apparatuur.

2.6.4 Cluster continuïteit

Privacy statements betreffende het cluster 'continuïteit'

1. Er worden regelmatig back-up kopieën van informatie gemaakt. Deze back-ups worden gedocumenteerd.
2. Er is beleid, voor vastgestelde procedures en de bijbehorende documentatie om het vereiste niveau van continuïteit voor informatiebeveiliging van Paraat scholen te kunnen waarborgen, ook bij calamiteiten.
3. Er is een vastgesteld beleid en procedures omtrent 'datalekken'. Datalekken worden aantoonbaar gecommuniceerd met het CvB.
4. Het beleid wordt jaarlijks geëvalueerd en er wordt verantwoording over afgelegd in het jaarverslag.

2.6.5 Cluster toegangsbeveiliging & integriteit

Privacy statements betreffende het cluster 'toegangsbeveiliging & integriteit'

1. Er is een beleid m.b.t. toegangsbeveiliging op basis informatiebeveiligingseisen (need-to-know).
2. Alle medewerkers hanteren een beveiligde inlogprocedure.

2.6.6 Cluster controle & logging

Privacy statements betreffende het cluster 'controle & logging'

1. De functionaris gegevensbescherming borgt en controleert de toegangsrechten van medewerkers regelmatig. Dit proces is cyclisch verankerd in een planning.
2. Het bestuur evalueert processen, beleid en afspraken jaarlijks en rapporteert hierover in het jaarverslag.

2.7 Controle & rapportage

Dit informatiebeveiligings- en privacy beleid wordt jaarlijks getoetst en bijgesteld door het College van Bestuur. Tevens wordt er jaarlijks verantwoording afgelegd met betrekking tot alles wat met privacy te maken heeft in het jaarverslag. Hierbij wordt rekening gehouden met:

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

2.8 Controle, naleving & sancties

Naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het AVG proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Paraat scholen wordt actief aandacht besteed aan AVG.
Voor de bevordering van de naleving van de Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt (in taak) aangewezen door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het CvB vast te stellen reglement. Mocht de naleving ernstig tekort schieten, dan kan Paraat scholen de betrokken verantwoordelijke medewerkers een disciplinaire maatregel op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij Paraat scholen is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

2.9 Classificatie & risico analyse

Bij Paraat scholen heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de 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 kwaliteitsaspecten die van belang voor de informatievoorziening.

2.10 Voorlichting & bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt 'de mens' meestal de belangrijkste speler. Daarom wordt bij Paraat scholen 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/voorlichting voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van directeuren, de FG (Functionaris Gegevensbescherming)(als taak), met het College van Bestuur als eindverantwoordelijke.

2.11 Datalekken

Deze paragraaf biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken. Gebruikte termen:

- **Beveiligingsincident:** een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening:** het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek:** een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene:** de persoon van wie de persoonsgegevens zijn gelekt.

2.11.1 Wet- & regelgeving datalekken

Op 1 januari 2016 is de voormalige wet bescherming persoonsgegevens gewijzigd. Door deze wijziging zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.
De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in je leerling administratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze verwerkers aanvullende afspraken maken over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van groep 3, is ook een datalek.

De meldplicht geldt voor de verwerkingsverantwoordelijke van de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een verwerker voor de school. Er kan worden afgesproken dat een verwerker namens de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

2.11.2 Afspraken met leveranciers

Het schoolbestuur moet als verwerkingsverantwoordelijke voor de persoonsgegevens, afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder (zie model verwerkersovereenkomst 3.0).
Wij spreken samen af:

- Hoe wij elkaar informeren over datalekken, en ervoor zorgen dat beide partijen bereikbaar zijn tijdens bijvoorbeeld het weekend en vakanties
- Wie de melding doet bij de Autoriteit Persoonsgegevens
- Welke informatiegegevens de bewerker moet geven bij een datalek
- Welke informatie nodig is voor het doen van een melding, en hoe wij elkaar informeren over de melding (maak afspraken dat ieder een kopie van de melding krijgt of doorstuurt)
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is

Het bovenstaande is beschreven in een protocol en maakt deel uit van deze notitie. Zie hiervoor ‘Tegeltje Wat Te Doen Bij Een Datalek’.

2.11.3 Vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker (medewerker):** degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.

2. **Meldpunt (servicedesk):** avg@paraatscholen.nl. Centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming):** degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus:** degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

2.11.4 Zeven stappen

Wij hanteren zeven stappen in het geval zich een datalek voordoet:

1. **Ontdekken**, de ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij de Functionaris Gegevensbescherming.
2. **Inventariseren**, de Functionaris Gegevensbescherming bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij / zij aanvullende vragen uit bij 'de ontdekker' en / of 'de technicus'. De volgende informatie wordt daarna vastgelegd:
    - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard).
    - Datum/periode van het beveiligingsincident.
    - Aard van het beveiligingsincident.
    - Wanneer van toepassing (bij een datalek):
        - omschrijving van de groep betrokkenen
        - aantal betrokkenen
        - type persoonsgegevens in kwestie
        - worden de gegevens binnen een keten gedeeld
3. **Beoordelen**, wanneer de Functionaris Gegevensbescherming voldoende informatie heeft verzameld en een datalek vermoedt, stuurt deze 'de melder' een verzoek om de verzamelde informatie te bekijken. De Functionaris Gegevensbescherming beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
   De volgende informatie wordt vastgelegd door de Functionaris Gegevensbescherming:
    - Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
    - Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens
    - Wordt het datalek aan betrokkenen gemeld
    - Hoe worden meldingen gedaan
    - Wat is de inhoud van de melding

   Bij de beoordeling of er sprake is van een 'melding plichtige datalek', wordt er rekening gehouden met het type gegevens en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden. Op het moment dat dit het geval is, schakelen wij, indien nodig de juridisch adviseur in van Paraat scholen.
4. **Repareren:** 'de technicus' wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus legt onderstaande vast:
    - Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
    - Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?
5. **Melden:** indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Functionaris Gegevensbescherming dit

binnen 72 uur doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpaee?Q .

6. **Vastleggen:** alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Functionaris Gegevensbescherming, waarmee het incident is afgesloten. De Functionaris Gegevensbescherming verstuurt een samenvatting van de genomen maatregelen aan 'de ontdekker'.
7. **Informeren betrokkene:** als de datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene, dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar).

2.11.5 Monitoring beveiligingsincidenten & datalekken

De Functionaris Gegevensbescherming maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken en bespreekt deze met het College van Bestuur.
In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

3 Rollen, verantwoordelijkheden & taken

Paraat scholen onderscheidt onderstaande rollen, verantwoordelijkheden en taken:

Niveau	Wie, Rollen	Hoe, Verantwoordelijkheid/taken	Wat, Realiseren/vastleggen
Richtinggevend (strategisch)	College van Bestuur	* Eindverantwoordelijk * IBP-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 * Reglement FG vaststellen * Privacyreglement vaststellen
Sturend (tactisch)	College van Bestuur	* Inhoudelijk verantwoordelijk voor AVG * AVG-planning en controle * Adviseert Raad van Toezicht over AVG * Voorbereiden uitvoeren AVG- beleid, classificatie/risicoanalyse * Hanteren AVG-normen en wijze van toetsen * Evalueren AVG-beleid en maatregelen * Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze * Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures AVG, waaronder: * Activiteitenkalender met bijvoorbeeld scholings- en voorlichtingsbijeen-komsten * Protocol beveiligingsincidenten en datalekken * Bewerkersovereenkomsten regelen * Toestemming gebruik foto's en video * Opstellen informatie documentatie richting leerlingen, ouders / verzorgers * Opstellen social media reglement * Opstellen gedragscode/protocol ICT en Internetgebruik * Opstellen gedragscode/protocol Medewerkers en leerlingen
	Functionaris voor Gegevens bescherming	* Toezicht op naleving privacywetgeving * Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens * Afwikkeling klachten en incidenten	* Privacyreglement, * Procedure IBP-incident afhandeling * Inrichten meldpunt datalekken
	Domeinverant-woordelijken ICT, beleidsmede werkers (HRM / P&O)	* Classificatie/risicoanalyse * Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren CvB * Toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	* Inventariseren waar persoons-gegevens van de school terechtkomen (leveranciers lijst) * Classificatie- en risicoanalyse documenten
Uitvoerend (operationeel)	Functionaris Gegevens bescherming	* Incidentafhandeling (registreren en evalueren). * Technisch aanspreekpunt voor AVG-incidenten. * Uitvoeren taken conform gegeven richtlijnen en procedures. * Verantwoordelijk omgaan met AVG bij hun dagelijkse werkzaamheden * communicatie naar alle betrokkenen, ervoor zorgen dat medewerkers op de hoogte zijn van het AVG-beleid en de consequenties ervan * toezien op de naleving van het AVG-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers	* Communiceren, informeren en toezien op naleving van o.a.: - AVG in het algemeen - Regels passend onderwijs - Hoe omgaan met leerling dossiers - Wie mogen wat zien - Gedragscode/protocollen - Omgaan met sociale media - Mediawijs maken * Rapporteren voortgang m.b.t. doelstellingen AVG-beleid aan bestuur

Vervolg Uitvoerend (operationeel)	Directie Medewerker	* Voorbeeldfunctie met positieve en actieve houding t.a.v. AVG-beleid * Implementeren AVG-maatregelen op bestuursniveau of schoolniveau * Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc. * Verantwoordelijk omgaan met AVG bij hun dagelijkse werkzaamheden	