Informatiebeveiligings- en privacy (IBP) beleid

DOMMELGROEP

cadans primair
leren beweegt ons

Versie 29-10-2019

DOMMELGROEP

Inhoudsopgave

DOMMELGROEP

Inleiding

Leerlingen hebben recht op een veilige leeromgeving en medewerkers op een veilige werkomgeving. Daar hoort ook bij dat hun privacy goed wordt beschermd. Privacy is niet zomaar iets: het is een grondrecht, net als het recht op vrijheid van godsdienst of het recht op vrijheid van meningsuiting. In de Universele Verklaring van de Rechten van de Mens is privacy geborgd als mensenrecht. In Europa is privacy vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens. En sinds 1983 is privacybescherming opgenomen in artikel 10 van de Nederlandse Grondwet. Artikel 8 van het Europees Handvest voor de Rechten van de Mens ziet specifiek toe op de bescherming van persoonsgegevens en luidt:

Artikel 8 Bescherming van persoonsgegevens
1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
*2. Deze gegevens moeten **eerlijk** worden verwerkt, voor **bepaalde doeleinden** en met toestemming van de betrokkene of op basis van een andere **gerechtvaardigde grondslag** waarin de wet voorziet. Eenieder heeft **recht op toegang** tot de over hem verzamelde gegevens en op **rectificatie** daarvan.*
3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

Vanaf 25 mei 2018 geldt voor alle landen van de EU de Algemene Verordening Gegevensbescherming (AVG). Daarin zijn basisbeginselen opgenomen waar iedere verwerking van persoonsgegevens aan moet voldoen. In Nederland geldt daarnaast de Uitvoeringswet op de AVG (UAVG) en diverse wetgeving waarin regels zijn opgenomen voor specifieke verwerkingen van persoonsgegevens. Relevante wetgeving is onder meer:

- Wet op het primair onderwijs
- Wet op het onderwijstoezicht
- Wet medezeggenschap op scholen
- Archiefwet
- Leerplichtwet
- Wetboek van Strafrecht

Om de privacy van de leerlingen en medewerkers te beschermen en een zorgvuldige verwerking van hun persoonsgegevens te waarborgen is een beleid over de omgang met persoonsgegevens noodzakelijk. In de AVG wordt dit het gegevensbeschermingsbeleid genoemd (art. 24 AVG). Dit Informatiebeveiligings- en privacy beleid (IBP beleid) is de vastlegging van dat beleid.

Dit IBP beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen (zoals leerlingen, medewerkers, ouders/verzorgers) wordt gerespecteerd en de Dommelgroep voldoet aan de relevante wet- en regelgeving.

DOMMELGROEP

Dit IBP beleid is opgesteld door de privacy-regiegroep van de Coöperatieve Dommelgroep U.A., waar 5 besturen deel van uitmaken en is ter goedkeuring voorgelegd aan de GMR-en en aan de 5 schoolbesturen van de Dommelgroep .

De GMR van CADANS PRIMAIR heeft ermee ingestemd op 29-10-2019.

Het bestuur van CADANS PRIMAIR heeft hiermee ingestemd op 29-10-2019.

Leeswijzer IBP Beleid en bijlagen

De opbouw van het IBP beleid is zo gekozen dat in de tekst van het document de algemene uitgangspunten zijn opgenomen van het IBP beleid binnen de Dommelgroep. Deze zijn gebaseerd op de geldende privacyregelgeving en geven weer op welke wijze deze binnen de Dommelgroep is geïmplementeerd. Daarnaast zijn de specifieke uitvoeringsdocumenten met de nadere concrete of praktische invulling van de uitvoering van de privacyregelgeving opgenomen in de bijlagen bij dit IBP beleid, dan wel wordt verwezen naar de vindplaats van deze documenten. Voor deze opzet is gekozen, omdat de bijlagen en de documenten waarnaar wordt verwezen regelmatig kunnen wijzigen als wijzigingen in de verwerking van de persoonsgegevens optreden. Om te voorkomen dat voor iedere wijziging in die uitvoeringsdocumenten het IBP beleid opnieuw zou moeten worden vastgesteld zijn deze opgenomen in afzonderlijke documenten. Indien een bijlage wijzigt zal dat via de ‘nieuwsbrief AVG’ worden aangegeven.

DOMMELGROEP

Hoofdstuk 1: Doel van informatiebeveiliging en privacy

1.1. Waarom is informatiebeveiliging en privacy belangrijk?

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.2. Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

Informatiebeveiliging richt zich op de volgende aspecten (zie ook hoofdstuk 4, paragraaf 1):

- *Beschikbaarheid*: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- *Integriteit*: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- *Vertrouwelijkheid*: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Het treffen van fysieke, procedurele, organisatorische en technische maatregelen is daarvoor van belang, maar de naleving is essentieel. Dit raakt zowel de professionaliteit van de individuele medewerker als de professionele cultuur als geheel. Om een beheersbare en betrouwbare informatievoorziening te behouden, is het van belang dat iedereen een aantal gemeenschappelijke uitgangspunten hanteert en deze uitdraagt. Er dient daarom constante aandacht te zijn voor het verhogen van het beveiligingsbewustzijn van al onze medewerkers en onze partners.

1.3. Toelichting privacy

Privacy ziet toe op de persoonlijke levenssfeer van ieder individu. Daarbij horen ook persoonsgegevens. De AVG regelt onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens mogen alleen verwerkt worden als dat gebaseerd is op een wettelijke grondslag, een gerechtvaardigd doel is vastgesteld, ervoor wordt gezorgd dat de gegevens juist zijn, deze niet langer worden bewaard dan nodig en passend worden beschermd. Daarbij geldt als

uitgangspunt dat niet meer persoonsgegevens mogen worden verwerkt dan noodzakelijk om de vastgestelde doelen te bereiken (‘dataminimalisatie’). Bovendien heeft ieder individu het recht om te weten wat er met zijn persoonsgegevens gebeurt en deze in te zien.

De AVG kent een verantwoordingsplicht. Dat betekent dat de verwerkingsverantwoordelijke moet kunnen aantonen dat wordt voldaan aan de beginselen van de verwerking van persoonsgegevens. De verwerkingsverantwoordelijke is de entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit IBP beleid is CADANS PRIMAIR, vertegenwoordigd door het College van Bestuur, de verwerkingsverantwoordelijke voor de verwerking van de persoonsgegevens van alle leerlingen en medewerkers.

1.4. Vervlechting informatiebeveiliging en privacy

Informatiebeveiliging is een belangrijke voorwaarde voor de bescherming van ieders privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit IBP-beleid vormt daarom de basis voor informatiebeveiliging en privacy binnen de Dommelgroep en vormt de kapstok voor alle afspraken en procedures over de omgang met en de bescherming van persoonsgegevens.

Hoofdstuk 2: Wat is de reikwijdte van dit IBP-beleid?

Relevante begrippen

Om een goede omgang met persoonsgegevens te kunnen waarborgen is het allereerst van belang dat er duidelijkheid bestaat over de relevante begrippen. De privacyregelgeving geldt voor iedere verwerking van persoonsgegevens. De begrippen persoonsgegeven en verwerking worden zeer ruim uitgelegd door de toezichthouders, waaronder de Autoriteit Persoonsgegevens.

Een *persoonsgegeven* is ieder gegeven dat herleidbaar is tot een natuurlijk persoon (de *betrokkene*), zoals een leerling, een medewerker of een ouder. Persoonsgegevens zijn bijvoorbeeld contactgegevens op een leerlingenlijst, alle gegevens in het LAS, rapporten, zorgplannen, een kopie van een paspoort van medewerkers en salarisgegevens.

Verwerking van persoonsgegevens is iedere handeling die betrekking heeft op persoonsgegevens. Het hoeft geen actieve handeling te zijn. Het kunnen inzien, bewaren, verstrekken of uitsluitend opslaan of vernietigen van persoonsgegevens valt allemaal onder het begrip verwerken.

Bijzondere persoonsgegevens zijn extra gevoelige persoonsgegevens die in principe niet verwerkt mogen worden. Het gaat onder meer om gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische (DNA/RNA) of biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, iemands seksueel gedrag of strafrechtelijke gegevens.

DOMMELGROEP

2.1. Op welke persoonsgegevens heeft dit IBP beleid betrekking?

Het IBP beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de Dommelgroep, waaronder in ieder geval alle medewerkers, leerlingen, ouders of verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan de Dommelgroep persoonsgegevens verwerkt.

2.2. Verwerkingsregisters

Het is niet mogelijk om te weten of wordt voldaan aan de privacyregelgeving, laat staan dat het mogelijk is om aan te tonen dat aan de AVG wordt voldaan als niet bekend is welke verwerkingen van persoonsgegevens plaatsvinden binnen de Dommelgroep. Op grond van artikel 30, lid 1 AVG is het verplicht om een verwerkingsregister bij te houden waarin de verwerkingen zijn opgenomen. Iedere verwerkingsverantwoordelijke zal in een verwerkingsregister moeten bijhouden welke categorieën van persoonsgegevens voor welke doelen worden verwerkt, wie de interne en externe ontvangers zijn van die gegevens, of gegevens buiten de EU worden verwerkt, welke bewaarcriteria gelden en welke beveiligingsmaatregelen zijn getroffen. Een deel van de verwerkingen vindt plaats op stichtingsniveau. Daarnaast worden persoonsgegevens verwerkt binnen de scholen van de stichtingen. Om een zo compleet mogelijk beeld te hebben en te voldoen aan de registerplicht van de AVG zijn vanuit de besturen van de Dommelgroep en de individuele scholen verwerkingsregisters gevuld met betrekking tot de diverse categorieën van betrokkenen. Iedere school zal onder begeleiding van de Functionaris van de Gegevensbescherming van de Coöperatie Dommelgroep U.A. (hierna: de FG) een verwerkingsregister vullen en onderhouden. Voor de stichting is een verwerkingsregister opgemaakt door de FG in overleg met het bestuurders.
De eerste categorie van betrokkenen zijn alle leerlingen van de scholen die vallen onder de Dommelgroep. Op stichtingsniveau vinden verwerkingen plaats van leerlinggegevens. Daarnaast vinden de meeste verwerkingen van leerlinggegevens plaats binnen de scholen. Deze registers van verwerkingsactiviteiten van de verwerkingen die betrekking hebben op persoonsgegevens van leerlingen worden bewaard op stichtingsniveau .

2.2.1. *Medewerkers*

De tweede categorie van betrokkenen zijn alle medewerkers in loondienst bij een bij de Dommelgroep aangesloten stichting. Op stichtingsniveau vinden de meeste verwerkingen plaats van deze gegevens, zoals de personeelsadministratie, de salarisadministratie en opleidingen. Bij de scholen worden persoonsgegevens van medewerkers met name voor praktische werkzaamheden verwerkt, zoals in het kader van de formatie, roosters en het taakbeleid. De registers van verwerkingsactiviteiten met betrekking tot medewerkers worden bewaard op stichtingsniveau.

2.2.2. *Ouders en/of verzorgers*

Niet alleen van de leerlingen, maar ook van hun ouders en/of verzorgers worden persoonsgegevens verwerkt op stichtingsniveau en met name binnen de scholen. Deze verwerkingen zijn opgenomen in de registers van de leerlingen.

DOMMELGROEP

2.2.3. *Overige betrokkenen*

Naast verwerkingen van leerlingen, medewerkers en ouders/verzorgers worden zowel binnen de stichtingen als op de scholen persoonsgegevens verwerkt van andere personen, zoals invalkrachten, uitzendkrachten, leveranciers van diverse (leer)middelen en externe zorgverleners. Deze verwerkingen zijn opgenomen op die plaatsen waar deze relevant zijn in het verwerkingsregister van leerlingen, dan wel die van medewerkers.

2.3. Begrenzing van de verwerking van persoonsgegevens

De ingevulde registers van verwerkingsactiviteiten vormen de begrenzing van de verwerking van persoonsgegevens binnen de Dommelgroep en de scholen die daaronder vallen. Op grond van de AVG dienen de doelen voor de verwerking van persoonsgegevens uitdrukkelijk te zijn omschreven en mogen niet meer gegevens worden verwerkt dan noodzakelijk is om die doelen te bereiken. De doelen en categorieën van persoonsgegevens staan omschreven in de verwerkingsregisters. Dat betekent dat de Dommelgroep en de onder haar verantwoordelijkheid vallende personen geen persoonsgegevens mogen verwerken die niet in de verwerkingsregisters zijn opgenomen. Tevens mogen de persoonsgegevens die beschikbaar zijn niet voor andere doelen worden verwerkt die niet verenigbaar zijn met de doelen die in de registers zijn opgenomen. De Dommelgroep zal zorgdragen voor bewustwording bij alle personen die de persoonsgegevens verwerken en onder haar verantwoordelijkheid vallen. Daarbij zal CADANS PRIMAIR in samenspraak met de directeuren van de scholen zorgen dat de leerkrachten, administratieve ondersteuners en andere betrokken personen werkinstructies krijgen in dat kader. Ook zal de Dommelgroep in de persoon van de FG erop toezien dat de feitelijke verwerkingen beperkt blijven door dat steekproefsgewijs te controleren. Met deze maatregelen wordt door de Dommelgroep geborgd dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk is voor de vastgestelde doelen.

DOMMELGROEP

Hoofdstuk 3: Rol en taken van CADANS PRIMAIR

3.1. Rol als verwerkingsverantwoordelijke

Als Verwerkingsverantwoordelijke zal ieder bestuur moeten voldoen aan de AVG en andere relevante wet- en regelgeving inzake de verwerking van persoonsgegevens. CADANS PRIMAIR neemt de verantwoordelijkheid om ervoor te zorgen dat de benodigde documenten worden opgesteld, de vereiste afspraken worden gemaakt met externe partijen en de personen die onder zijn verantwoordelijkheid persoonsgegevens verwerken voldoende instructies en informatie verkrijgen om een passende bescherming van de persoonsgegevens te waarborgen. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. Een goede balans tussen het belang van ieder bestuur om persoonsgegevens te verwerken en het belang van de betrokkenen voor de bescherming van zijn/haar persoonsgegevens wordt voorop gesteld. In het privacyreglement in **bijlage 1** heeft de Dommelgroep de uitgangspunten voor de omgang met persoonsgegevens op een rij gezet.

3.2. Taken en verantwoordelijkheden

De Dommelgroep heeft de taak en de verantwoordelijkheid om een zorgvuldige omgang met persoonsgegevens en de naleving van de AVG en andere relevante regelgeving te waarborgen.
In dat kader is vanuit de Dommelgroep een privacy-regiegroep aangesteld om de verdere implementatie van de AVG en aanverwante privacyregelgeving binnen de schoolbesturen die deelnemen aan de Coöperatieve Dommelgroep U.A te coördineren. Daarnaast maken de schoolbesturen die deel uitmaken van Coöperatieve Dommelgroep U.A., gezamenlijk gebruik van een FG.
Onder leiding van de FG is er ook een groep contactpersonen AVG. In deze groep is CADANS PRIMAIR met één persoon vertegenwoordigd. Deze groep vormt ook een ‘denktank AVG’.

3.2.1 *Voorlichting en bewustwording binnen de organisatie*

Beleid en maatregelen zijn niet voldoende om persoonsgegevens passend te beschermen. De feitelijke omgang met persoonsgegevens door alle personen die werkzaam zijn voor of onder de verantwoordelijkheid vallen van de Dommelgroep dient zorgvuldig te zijn en in overeenstemming met de AVG. Dat betekent dat al deze personen de persoonsgegevens die zij verwerken, geheim dienen te houden. Dit wordt geregeld d.m.v. een geheimhoudingsverklaring**.** Zie **bijlage 9**.
Om dit te bevorderen zorgt de Dommelgroep met hulp van de FG voor diverse bewustwordingscampagnes voor medewerkers. Zowel via nieuwsbrieven als in workshops (per groep gebruikers), wordt aandacht gegeven aan de relevantie van een zorgvuldige omgang met persoonsgegevens en wat zorgvuldige omgang inhoudt. Ook ouders worden geïnformeerd via nieuwsbrieven. Daarmee wordt het bewustzijn van de medewerkers voortdurend aangescherpt, zodat de kennis van risico’s wordt verhoogd en veilige en verantwoorde omgang met persoonsgegevens wordt aangemoedigd.

Verhoging van het IBP-bewustzijn binnen de Dommelgroep is een gezamenlijke verantwoordelijkheid van de FG, de contactpersoon AVG en ieder bestuur.

3.2.2. *Handreiking AVG*

Binnen de Dommelgroep is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, zoals met sterke wachtwoorden of wachtzinnen, maar ook de bescherming van papieren documenten. Daarnaast zijn er afspraken over het gebruik van internet en sociale media. De Dommelgroep heeft een handreiking die specifiek toeziet op een veilige omgang met persoonsgegevens. Deze handreiking is opgenomen in **bijlage 5** en wordt na een gezamenlijke workshop digitaal verspreid onder alle medewerkers.

3.2.3. *Verdeling van verantwoordelijkheden*

Ieder bestuur is op grond van haar rol als verwerkingsverantwoordelijke eindverantwoordelijk voor de naleving van de privacyregelgeving. CADANS PRIMAIR heeft echter geen direct zicht op de verwerkingen die zich afspelen bij de individuele scholen. Naast de hiervoor genoemde regiegroep, contactpersonen en FG hebben meerdere personen een concrete rol met daarbij horende taken met betrekking tot de naleving van deze regelgeving. Een overzicht van deze rollen en taken is opgenomen in **bijlage 2**.

3.2.4. *Functionaris voor de Gegevensbescherming (FG)*

De FG levert een bijdrage aan het ontwikkelen, bewaken en evalueren van de procedures, planningen en instrumenten in het kader van de AVG. De FG houdt tevens toezicht op de naleving van de AVG. De FG verricht zijn werkzaamheden binnen de Coöperatieve Dommelgroep U.A. en rapporteert jaarlijks aan ieder bestuur. De functiebeschrijving van de FG bevindt zich in **bijlage 3**.

Hoofdstuk 4: Informatiebeveiliging en meldplicht datalekken

4.1. Classificatie en risicoanalyse

De AVG schrijft voor dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen dient te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij de beoordeling van het passende beveiligingsniveau dient met name rekening te worden gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde toegang tot persoonsgegevens (artikel 32 AVG). Alle gegevens en informatiesystemen waarop dit IBP beleid van toepassing is, wordt geclassificeerd om te bepalen welke beveiligingsmaatregelen passend zijn. Het niveau van de te nemen beveiligingsmaatregelen is namelijk afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het concrete informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn

beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn. De classificatie is opgenomen in de verwerkingsregisters.

4.1.1. *Plan-do-check-act cyclus*

Om de beveiliging van persoonsgegevens passend te houden zal op gezette tijden getest, beoordeeld en geëvalueerd moeten worden of de getroffen maatregelen doeltreffend zijn of dat aanpassing vereist is. De maatregelen die getroffen zijn, zijn opgenomen in de rapportages van de FG. Deze worden bewaard op bestuursniveau.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen zal vóóraf gekeken moeten worden naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging, zodat passende maatregelen genomen kunnen worden. Zo zal vanaf de start van nieuwe (ICT)projecten rekening moeten worden gehouden met informatiebeveiliging.
Om de privacyrisico's van een gegevensverwerking in kaart te brengen, kan een data protection impact assessment (DPIA) worden uitgevoerd. Hierna kunnen maatregelen worden getroffen om deze risico's te verkleinen.

4.1.2. *Logging en monitoring*

Geautomatiseerde systemen worden automatisch gelogd en gemonitord en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (pogingen) tot ongeautoriseerde toegang tot het netwerk.

4.2. Meldplicht beveiligingsincidenten en datalekken

Een *beveiligingsincident* is een gebeurtenis waarbij de mogelijkheid bestaat dat de beveiliging van informatie of informatieverwerkende systemen in gevaar is of kan komen.
Een *datalek* is een beveiligingsincident; waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt, zoals het sturen van een e-mail met leerlingenlijst naar de verkeerde ontvanger of het verlies van een USB stick met een personeelsdossier. Een datalek dient gemeld te worden aan de Autoriteit Persoonsgegevens, tenzij het datalek geen risico's inhoudt voor de betrokkene(n). Tevens dient de verwerkingsverantwoordelijke de betrokkene(n) te informeren indien het datalek een groot risico inhoudt voor de betrokkene(n). Bijvoorbeeld bij het lekken van inloggegevens of gegevens die gebruikt kunnen worden om identiteitsfraude te plegen (BSN of kopie ID-bewijs).

4.2.1. *Procedure beveiligingsincidenten en meldplicht datalekken*

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden bij hun directeur. Het melden van datalekken is vastgelegd in een protocol dat is opgenomen in **bijlage 6**.
Voor afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Periodiek zullen de datalekken besproken worden met het CvB en de FG.

DOMMELGROEP

Hoofdstuk 5: Afspraken met derden

5.1. Overzicht van derden en de rol van deze derden

De AVG en ook de overige privacyregelgeving maakt een onderscheid tussen twee rollen, namelijk de *verwerkingsverantwoordelijke* en de *verwerker*. Zoals in hoofdstuk 3 toegelicht geldt ieder bestuur als verwerkingsverantwoordelijke in de zin van de AVG en zal zij moeten voldoen aan alle vereisten van de privacyregelgeving.

De *verwerker* is degene die persoonsgegevens verwerkt *ten behoeve van* een verwerkingsverantwoordelijke. Een verwerker heeft geen eigen doel voor de verwerking van de persoonsgegevens buiten het uitvoeren van de dienstverlening voor het bestuur. Een verwerker heeft op grond van de privacywetgeving veel minder verplichtingen. Een verwerker dient de persoonsgegevens geheim te houden, mag deze niet voor een ander doel verwerken dan in het kader van de opdracht van de verwerkingsverantwoordelijke en zal moeten zorgdragen voor een passende beveiliging van de persoonsgegevens. Een verwerker heeft echter onder meer geen eigen grondslag of doel voor de verwerking nodig, heeft geen informatieplicht richting betrokkenen, hoeft geen datalekken te melden bij de Autoriteit Persoonsgegevens en hoeft niet rechtstreeks te reageren op verzoeken van betrokkenen. Ieder bestuur blijft verantwoordelijk voor de juiste omgang met de persoonsgegevens, ook als bepaalde verwerkingen worden uitbesteed aan een verwerker. Zie hiervoor de betreffende verwerkersovereenkomsten.

De verwerkers waar de Dommelgroep gebruik van maakt voor haar scholen zijn onder meer de leveranciers van digitale leermiddelen, het leerling-administratiesysteem, de leerlingvolgsystemen en de beheerder van de digitale infrastructuur binnen alle scholen. Daarnaast maakt de Dommelgroep gebruik van partijen die de personeelsadministratie onderhouden en beheren en partijen die worden ingeschakeld in het kader van de werving- en selectie van nieuwe medewerkers voor de Dommelgroep. De partijen waarmee de Dommelgroep met alle scholen gegevens uitwisselen worden opgenomen in de betreffende verwerkingsregisters.

5.1.1. *Afspraken met verwerkers*

Indien een bestuur verwerkers inschakelt zal zij een verwerkersovereenkomst moeten sluiten met deze partijen. De PO-Raad, de VO-raad, MBO-raad en leden van brancheorganisaties en verschillende leveranciers van digitale onderwijsmiddelen en informatiesystemen hebben het Convenant Digitale Onderwijsmiddelen en Privacy 3.0 afgesloten. Dit convenant is in overeenstemming met de vereisten van de AVG opgesteld en bevat als bijlage een Model Verwerkersovereenkomst. Indien een bestuur gebruik maakt van de diensten van verwerkers volgt zij de richtlijnen en adviezen van de PO-raad en sluit met deze partijen de verwerkersovereenkomst conform genoemd model. De gesloten verwerkersovereenkomsten worden door de FG bijgehouden bij het verwerkingsregister en worden bewaard op bestuursniveau.

5.1.2. *Afspraken met andere partijen*

Het kan ook voorkomen dat de derde waarmee persoonsgegevens worden uitgewisseld of die persoonsgegevens verwerkt voor de Dommelgroep, een bepaalde zeggenschap heeft over de verwerking van deze gegevens. Zoals een zorgverlener die een leerling begeleidt of de bedrijfsarts die een zieke medewerker op spreekuur krijgt. In dat geval is die derde ook een verwerkingsverantwoordelijke en geen verwerker. Het convenant of de verwerkersovereenkomst zijn dan niet van toepassing.

Indien de andere partij gezamenlijk met een bestuur het doel voor de gegevensverwerking bepaalt zijn partijen gezamenlijke verwerkingsverantwoordelijken en zullen zij op grond van artikel 26 AVG een regeling moeten vastleggen over de omgang met persoonsgegevens. Als de andere partij andere doelen heeft voor de verwerking van persoonsgegevens dan een bestuur, gelden beide partijen als afzonderlijke verwerkingsverantwoordelijken. Er is geen wettelijke verplichting opgenomen in de AVG voor het sluiten van een overeenkomst tussen twee afzonderlijke verwerkingsverantwoordelijken.

Voor de gegevensuitwisseling met andere partijen kan worden gewerkt met een online registratiesysteem (zoals Parnassys, Esis of Eduscope). Er is dan beperkte autorisatie mogelijk. Ouders hebben inzage en correctierecht.
Ieder bestuur zal ten aanzien van de door haar ingeschakelde derden samen met de FG bepalen welke rol die hebben, óf en welke afspraken gemaakt moeten worden en houdt dit bij in het verwerkingsregister.

5.2. **Verdeling taken voor het maken van afspraken tussen bestuur en de school**

Ieder bestuur maakt een overzicht van de partijen waarmee verwerkersovereenkomsten gesloten moeten worden. Dat geldt in ieder geval voor die partijen die diensten aan besturen verlenen of aan meerdere scholen. Daarnaast zal het voorkomen dat scholen specifieke diensten uitbesteden aan derde partijen. Bijvoorbeeld in het kader van specifieke activiteiten die door de school worden aangeboden, zoals een fotograaf of leverancier van oudertevredenheidsonderzoeken. Omdat het zowel voor de school als voor een bestuur niet werkbaar is dat het bestuur dan zelf een verwerkersovereenkomst sluit met die partijen, geldt op grond van de algemene mandatering, dat indien de directeur een dergelijke verwerkersovereenkomst afsluit, dit geschiedt namens het bestuur.

DOMMELGROEP

Hoofdstuk 6: Transparantie en rechten betrokkenen

6.1. Informeren ouders, kinderen en medewerkers

Iedere betrokkene heeft het recht om te weten welke persoonsgegevens van hem worden verwerkt, voor welke doeleinden, wie de ontvangers zijn, wat hun rechten zijn, etc. Dit brengt mee dat de Dommelgroep de verplichting heeft om de betrokkenen daarover te informeren. De ouders moeten helder en begrijpelijk worden geïnformeerd over de omgang met de persoonsgegevens van hun kinderen en van henzelf. De Dommelgroep heeft daarvoor een privacyverklaring op de website geplaatst en op alle websites van de scholen zal op de homepage dezelfde privacyverklaring moeten staan. De ouders en/of verzorgers van de leerlingen zullen op die verklaring worden gewezen d.m.v. de schoolgids.

Ook de medewerkers moeten helder en begrijpelijk worden geïnformeerd over de omgang met hun persoonsgegevens**.** Zie de privacyverklaring voor medewerkers, **bijlage 1.**

6.2. Werkwijze voor rechten betrokkenen

Onder de AVG hebben betrokkenen een recht op inzage, correctie, 'recht op vergetelheid', het recht op afscherming van hun persoonsgegevens, recht van bezwaar en het recht op overdracht van persoonsgegevens. Buiten het recht op inzage en correctie gelden de andere rechten niet altijd. In de privacyverklaring worden de betrokkenen gewezen op deze rechten. Daarbij geldt als uitgangspunt dat bij een dergelijk verzoek de medewerker die het verzoek binnenkrijgt deze doorgeeft aan de directeur van de school waar de medewerker werkzaam is. De directeur zal het verzoek in samenspraak met de FG behandelen. Indien de medewerker bij de stichting werkzaam is zal deze het verzoek doorsturen aan de FG.

Hoofdstuk 7: Rol (Gemeenschappelijke) Medezeggenschapsraad

De gemeenschappelijke medezeggenschapsraden binnen de Dommelgroep hebben op grond van de Wet medezeggenschap op scholen instemmingsrecht over een regeling met betrekking tot de verwerking of de bescherming van persoonsgegevens. Meer specifiek hebben de oudergeledingen instemmingsrecht inzake regelingen over de verwerking van leerlinggegevens of gegevens van ouders en de personeelsgeledingen hebben instemmingsrecht inzake regelingen over de verwerking van gegevens van medewerkers.

Naast de GMR-en is de MR van iedere school een goede partner voor directie en team om te bespreken op welke wijze de school de privacybescherming vorm geeft. Ook kan een (G)MR (ongevraagd) advies geven naar aanleiding van vragen of klachten van ouders of medewerkers over de privacy op school of binnen de stichting.

DOMMELGROEP

Hoofdstuk 8: Specifieke onderwerpen

8.1 Gebruik beeldmateriaal (foto's en video's).

Om deze gegevens van leerlingen te mogen publiceren is toestemming van de ouders en/of verzorgers vereist. De Dommelgroep heeft het toestemmingsformulier aangepast aan de AVG en de informatie van de Autoriteit Persoonsgegevens hierover. Dit formulier bevindt zich in **bijlage 7** bij dit IBP beleid. Iedere school zal jaarlijks toestemming vragen voor het gebruik van de genoemde gegevens aan de hand van dit formulier en zal ervoor zorgdragen dat er geen gegevens van leerlingen worden gepubliceerd waarvoor geen toestemming is verkregen.

8.2 Email en telefoonnummers.

Voor sociale doeleinden wordt ook toestemming gevraagd voor het verspreiden van leerlingenlijsten. Hierop staan emailadressen en telefoonnummers. Hiervoor wordt éénmalig toestemming gevraagd. Zie **bijlage 8**. (Deze toestemming kan ook reeds zijn opgenomen in het aanmeldformulier).
Voor uitwisseling van persoonsgegevens voor onderwijsdoeleinden hoeft geen toestemming te worden gevraagd. Hiervoor geldt namelijk een gerechtvaardigd belang.

8.3 **Privacy bij extra begeleiding en zorg**

De Dommelgroep met alle scholen kan voor de begeleiding van leerlingen en ouders/verzorgers samenwerken met partners. Daarbij kunnen (bijzondere) persoonsgegevens worden gedeeld. Voor de verwerking van bijzondere persoonsgegevens bestaat een verbod, tenzij daar een wettelijke uitzondering voor bestaat. Zo mogen gegevens over de gezondheid van leerlingen door school worden verwerkt indien dat noodzakelijk is voor de speciale begeleiding van leerlingen of voor het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand (artikel 30 lid 2 UAVG). Bijvoorbeeld in geval van specifieke beperkingen, epilepsie of ernstige allergieën, dan wel extra begeleiding in verband met dyslexie. Ieder bestuur sluit aan bij het privacybeleid van het Samenwerkingsverband Passend Onderwijs.

8.4. Privacy bij overstapdossiers

In de wet is het belangrijkste uitgangspunt dat scholen altijd vooraf aan de uitwisseling moeten afwegen welke specifieke gegevens van iedere leerling daadwerkelijk nodig zijn ten behoeve van het leren en begeleiden van een leerling bij een nieuwe stichting. Dit betekent dat er per leerling die overstapt, moet worden bepaald welke gegevens relevant en proportioneel zijn. Gegevens die niet aan dit criterium voldoen, mogen niet door scholen uitgewisseld worden (hoe handig het doorgeven van die informatie ook lijkt). Welke gegevens dit zijn wordt afgesproken en bepaald binnen de besturen van de betreffende scholen.
Uitgangspunt: alleen opnemen wat wettelijk verplicht is. Zie **bijlage 10**.
In het "Besluit uitwisseling leer- en begeleidingsgegevens" is namelijk bepaald welke gegevens mogen worden opgenomen in het onderwijskundig rapport. Deze regels en de beperkte set gegevens die volgens dit Besluit mogen worden uitgewisseld vormen de basisvoorwaarde voor een

transparante elektronische uitwisseling van gegevens tussen scholen, waarbij de kans op fouten zo klein mogelijk is en de privacy van de betrokkenen gewaarborgd is.
Ook zijn de onderwijswetten van toepassing. In artikel 42 van de Wet op het primair onderwijs is vastgesteld dat een directeur van een school verplicht is om een onderwijskundig rapport op te stellen en te verstrekken aan de nieuwe school. Ook moeten de ouders / verzorgers een afschrift krijgen. Bezwaren van ouders en/of verzorgers zullen opgenomen moeten worden.

Ieder bestuur draagt er zorg voor dat alle schooldirecteuren op de hoogte zijn van deze regels.

Hoofdstuk 9: Evaluatie en wijzigingen

9.1. Afspraken over evaluatiemomenten en doorvoeren wijzigingen

Dit IBP beleid wordt minimaal elke twee jaar in het kader van de Risico Inventarisatie en Evaluatie (RI&E) getoetst en bijgesteld door de FG. De AVG is een apart onderdeel binnen de RI&E. Hierbij wordt rekening gehouden met:

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

Indien nodig zal het IBP beleid worden aangepast. Bij substantiële aanpassingen zal het aangepaste IBP beleid ter goedkeuring worden voorgelegd aan de GMR. Daarnaast kent de Dommelgroep een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy op bestuursniveau. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP beleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving en andere relevante ontwikkelingen meegenomen.
Deze jaarlijkse evaluatie vindt plaats in samenspraak met de contactpersonen AVG.

9.2. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Daarnaast wordt er tweejaarlijks een 'Checklist AVG' ingevuld op schoolniveau en op bestuursniveau. Van belang hierbij is dat iedereen zijn verantwoordelijkheid neemt en anderen aanspreekt in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met periodieke bewustwordingscampagnes, etcetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. Mocht de naleving van dit IBP beleid ernstig tekort schieten, dan kan een bestuur de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

DOMMELGROEP

Bijlage 1: Privacyreglement en Privacyverklaring

Privacyreglement voor CADANS PRIMAIR

1. Toepasselijkheid	Dit reglement geldt voor de gehele organisatie die deel uitmaakt van CADANS PRIMAIR. CADANS PRIMAIR is gevestigd op Schildershof 1A te Sint-Michielsgestel.
2. Definities	
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto's, video's, IP-adressen, tracking cookies, loginnamen en wachtwoorden.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Bijzondere persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto's) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.
Wettelijk vertegenwoordiger	Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd. Als een leerling 16 jaar of ouder is, beslist hij in voorkomende gevallen zelf over zijn privacy.
Verwerkingsverantwoordelijke	De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is CADANS

	PRIMAIR, vertegenwoordigd door het College van Bestuur, de verwerkingsverantwoordelijke.
Verwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke (CADANS PRIMAIR) persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerling-administratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken.
CADANS PRIMAIR	CADANS PRIMAIR, de verwerkingsverantwoordelijke in de zin van dit reglement.
3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers). 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door CADANS PRIMAIR worden verwerkt. Het reglement heeft tot doel: a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens; b. vast te stellen met welk doel en op welke (juridische) grondslag persoonsgegevens binnen CADANS PRIMAIR worden verwerkt; c. ook overigens te borgen dat persoonsgegevens binnen CADANS PRIMAIR rechtmatig, transparant en behoorlijk worden verwerkt; d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten door CADANS PRIMAIR worden gerespecteerd.
4. Doelen van de verwerking van persoonsgegevens	Bij de verwerking van persoonsgegevens houdt CADANS PRIMAIR zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving.
Doelen	1. De verwerking van persoonsgegevens vindt plaats voor:

	a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van studieadviezen; b. het verstrekken en/of ter beschikking stellen van leermiddelen; c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers; d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede van informatie over de leerlingen op de eigen website; e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van CADANS PRIMAIR of van de scholen, in brochures, ouderbrieven, de schoolgids of via social media; f. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen; g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole; h. het onderhouden van contacten met oud-leerlingen; i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers; j. de uitvoering of toepassing van wet- en regelgeving; k. juridische procedures waarbij CADANS PRIMAIR betrokken is. 2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.
5. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. CADANS PRIMAIR verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken.
6. Soorten persoonsgegevens	De categorieën van persoonsgegevens zoals deze binnen CADANS PRIMAIR worden verwerkt, worden geregistreerd in een verwerkingsregister.
7. Grondslag verwerking	Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan: a. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan CADANS PRIMAIR is opgedragen. b. De verwerking is noodzakelijk om te voldoen aan een wettelijke

	verplichting die op CADANS PRIMAIR rust. c. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. d. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van CADANS PRIMAIR of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is; in het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden. e. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang). f. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
8. Bewaartermijnen	CADANS PRIMAIR bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is. Binnen de organisatie van CADANS PRIMAIR geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan: a. de verwerker die van CADANS PRIMAIR de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken; b. derden voor zover uit de wet voortvloeit dat CADANS PRIMAIR verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang.
9. Beveiliging en geheimhouding	1. CADANS PRIMAIR neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens (zowel digtiaal als op papier) worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen.

2. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen.
3. Een ieder die betrokken is bij de verwerking van persoonsgegevens binnen CADANS PRIMAIR is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de uitoefening van de betreffende functie, werkzaamheden of taak.

10. Verstrekken gegevens aan derden

CADANS PRIMAIR kan persoonsgegevens aan derden verstrekken als daarvoor een grondslag bestaat in de zin van artikel 7 van dit reglement.

11. Sociale media

Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het sociale mediaprotocol van CADANS PRIMAIR.

12. Rechten betrokkenen

1. CADANS PRIMAIR erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:

Inzage

a. Een betrokkene heeft recht op inzage van de door CADANS PRIMAIR verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor zover het gaat om interne notities, die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en vrijheden van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan CADANS PRIMAIR het recht op inzage beperken.

   Bij het verstrekken van de betreffende gegevens verschaft CADANS PRIMAIR voorts informatie over:
- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens die worden verwerkt;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- (indien van toepassing) ontvangers in derde landen of internationale organisaties;
- (indien mogelijk) hoe lang de gegevens worden bewaard;
- dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij

het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens;
- het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens;
- de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen;
- het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene;
- de passende waarborgen indien de persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie.

Verbetering, aanvulling, verwijdering

b. CADANS PRIMAIR verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en CADANS PRIMAIR vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. CADANS PRIMAIR gaat daartoe over indien is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.

Bezwaar

c. Indien CADANS PRIMAIR persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt CADANS PRIMAIR de verwerking van de betreffende persoonsgegevens, behalve als naar het oordeel van CADANS PRIMAIR het belang van CADANS PRIMAIR, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt.

Beperken verwerking

d. De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. CADANS PRIMAIR staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, CADANS PRIMAIR de gegevens nodig heeft voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen.

Kennisgevingsplicht	e. Als CADANS PRIMAIR op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal CADANS PRIMAIR eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.
Procedure	2. CADANS PRIMAIR handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer CADANS PRIMAIR geen gevolg geeft aan het verzoek van de betrokkene, deelt CADANS PRIMAIR onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.
Intrekken toestemming	3. Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijden door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt CADANS PRIMAIR de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.
13. Transparantie	CADANS PRIMAIR informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld: a) de contactgegevens van CADANS PRIMAIR; b) de contactgegevens van de functionaris voor gegevensbescherming van CADANS PRIMAIR; c) de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking; d) een omschrijving van de belangen van CADANS PRIMAIR indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van CADANS PRIMAIR;

	e) de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden; f) in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER); g) hoe lang de persoonsgegevens zullen worden bewaard; h) dat de betrokkene het recht heeft om CADANS PRIMAIR te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid; i) dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming; j) dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens; k) of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt; l) het bestaan van geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
14. Meldplicht datalekken	Een ieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het meldpunt (fg@dommelgroep.nl) conform het protocol beveiligingsincidenten en datalekken van CADANS PRIMAIR. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt. Bijvoorbeeld door het laten rondslingeren van wachtwoorden, usb-stick / externe harde schijf of lijsten met leerlinggegevens.
15. Klachten	1. Wanneer een betrokkene van mening is dat het doen of nalaten van CADANS PRIMAIR niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen CADANS PRIMAIR geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van CADANS PRIMAIR. 2. Als een klacht naar de mening van betrokkene door CADANS PRIMAIR niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.

DOMMELGROEP

16. Onvoorziene situatie	Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt het College van Bestuur van CADANS PRIMAIR de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.
17. Wijzigingen reglement	1. Dit reglement is na instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) vastgesteld door het College van Bestuur van CADANS PRIMAIR. Het reglement wordt gepubliceerd op de website van CADANS PRIMAIR en de websites van de scholen. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids. 2. Het College van Bestuur kan dit reglement wijzigen na instemming van de GMR.
18. Slotbepaling	Dit reglement wordt aangehaald als het privacyreglement van CADANS PRIMAIR en treedt in werking op 29 oktober 2019.

Privacyverklaring voor ouders:
CADANS PRIMAIR en de Algemene Verordening Gegevensbescherming (AVG).

Contactgegevens: CADANS PRIMAIR, Schildershof 1A te Sint-Michielsgestel.
Contactgegevens Functionaris voor Gegevensbescherming: fg@dommelgroep.nl

Onze scholen verwerken persoonsgegevens van u en uw kinderen. CADANS PRIMAIR is wettelijk verantwoordelijk. CADANS PRIMAIR vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving. We leggen u graag uit hoe wij met de persoonsgegevens van uw kind omgaan.

Waarom verwerken wij gegevens van uw kind?
CADANS PRIMAIR verwerkt persoonsgegevens van uw kind om onze verplichtingen als onderwijsinstelling te kunnen nakomen. Zo hebben wij bijvoorbeeld de gegevens nodig om uw kind aan te melden als leerling op onze school en om de voortgang bij te houden. Daarnaast hebben wij de wettelijke verplichting om bepaalde gegevens door te sturen naar andere partijen, zoals DUO (ministerie van Onderwijs) en leerplicht.
Wij verwerken gegevens van uw kind voor het uitvoeren van de *onderwijsovereenkomst* die we met uw kind hebben en/of voor het nakomen van onze *wettelijke verplichtingen.*
Gegevens die hier niet aan voldoen zullen wij alleen met uw toestemming verwerken. Als voor het verwerken van gegevens toestemming wordt gevraagd zoals voor het gebruik van beeldmateriaal (foto's en video's) en verspreiding van emailgegevens en telefoonnummers, dan kunt u de

toestemming op elk moment intrekken of alsnog geven. (Wijziging van toestemming is niet van toepassing op inmiddels gepubliceerd beeldmateriaal).

Welke gegevens verwerken wij van uw kind?

Wij verwerken diverse soorten gegevens, waarvan wij de meeste gegevens rechtstreeks van u als ouders hebben gekregen. U kunt hierbij denken aan contactgegevens en geboorteplaats. Als u weigert de voor ons noodzakelijke gegevens te verstrekken, kunnen wij onze verplichtingen niet nakomen. De verstrekking van deze gegevens is dan ook een voorwaarde om uw kind bij ons in te kunnen schrijven. Wij verwerken ook medische gegevens van uw kind indien dat noodzakelijk is voor de juiste onderwijskundige, specifieke begeleiding. Ook verwerken wij medische gegevens als die nodig zijn om in noodgevallen goed te kunnen handelen.

Welke persoonsgegevens wij van uw kind verwerken vindt u hieronder:

Categorie	Toelichting
1. Contactgegevens	1a: naam, voornaam, e-mail, opleiding; 1b: geboortedatum, geslacht; 1c: overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen.
2. Leerlingnummer	een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1
3. Nationaliteit en Geboorteplaats	
4. Ouders, voogd	contactgegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres).
5. Medische gegevens	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen.
6. Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het te volgen onderwijs (bijvoorbeeld: leerling vrij op bepaalde dag).
7.Voortgang	gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: • Toetsen • Begeleiding leerling (inclusief ontwikkelperspectief OPP) • Aanwezigheidsregistratie • Medisch dossier • Klas/groep, leerjaar

8. Onderwijsorganisatie	gegevens met het oog op het organiseren van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen.
9. Financiën	gegevens voor het berekenen, vastleggen en innen van bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten (denk hierbij aan een bankrekeningnummer van de ouders).
10. Beeldmateriaal	foto's en videobeelden (met of zonder geluid) van activiteiten van de school op basis van toestemming. Let op: Voor pasfoto voor identificatiedoeleinden is geen toestemming nodig; als aanvulling op het dossier.
11. Leraar /zorgcoördinator/ intern begeleider/	gegevens van leraren en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van de instelling en het geven van onderwijs.
12. BSN (PGN)	In het onderwijs heet het BSN het persoonsgebonden nummer (PGN). Ook wel onderwijsnummer genoemd. Het PGN is hetzelfde nummer als het BSN. Scholen zijn verplicht het PGN te gebruiken in hun administratie.
13. Keten-ID (Eck-Id)	unieke iD voor de 'educatieve contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of leraren.
14 Overige gegevens, te weten ….	andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een andere wet. Deze zullen apart vermeld en toegelicht worden.

Hoe gaan wij om met de gegevens van uw kind?
Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid, wij zullen niet meer gegevens verwerken dan noodzakelijk is om onze rechten en plichten als onderwijsinstelling na te komen. Dit betekent ook dat we de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen.

In een aantal gevallen zijn wij, zoals eerder aangegeven, verplicht om gegevens van uw kind te delen met andere organisaties. Dit zijn onder andere DUO, leerplicht, de onderwijsinspectie, GGD/schoolarts, samenwerkingsverband en accountant.

Wij kunnen commerciële derde partijen verzoeken om te ondersteunen bij het verwerken van de gegevens voor de eerder genoemde doeleinden. Denk hierbij aan applicaties om leerlingen in de les te ondersteunen, een administratiesysteem waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie of een lesroosterprogramma. Dit gebeurt altijd in opdracht en onder de verantwoordelijkheid van CADANS PRIMAIR. Met deze organisaties sluiten we overeenkomsten af, waarin o.a. is vastgelegd welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden.

DOMMELGROEP

Wij zullen de gegevens van uw kind niet delen met commerciële derde partijen voor andere doeleinden. Ook zullen wij de gegevens van uw kind nooit verkopen of verhuren aan derde partijen.

De persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen die medewerkers kunnen bij de gegevens, die dat ook voor de uitvoering van hun werk nodig hebben. Daarnaast bewaren wij de gegevens niet langer dan noodzakelijk is. Wij hanteren hiervoor verschillende bewaartermijnen die wettelijk geregeld en vastgesteld zijn. Gegevens uit de leerling-administratie worden over het algemeen 7 jaar bewaard.

Welke rechten hebben ouders van leerlingen jonger dan 16 jaar?
Als ouders heeft u een aantal rechten als het gaat om persoonsgegevens. Deze rechten zijn in de wet vastgelegd. Ouders kunnen op elk moment gebruik maken van deze rechten. Dit betekent bijvoorbeeld dat u altijd een verzoek kunt indienen om inzage te krijgen in de gegevens die wij van uw kind verwerken.
Daarnaast kunt u ook een verzoek indienen om gegevens te rectificeren, te beperken of helemaal te wissen uit de systemen van de school. U heeft altijd het recht om onjuiste gegevens aan te vullen of te verbeteren. Als u ons verzoekt om gegevens van uw kind te beperken of te wissen, zullen wij toetsen of dit mogelijk is. In deze toets houden wij ons aan de wettelijke voorschriften en kijken wij bijvoorbeeld of wij geen wettelijke plicht hebben om de gegevens te bewaren.
Tevens heeft u het recht om te vragen om de gegevens, die wij van uw kind verwerken en wij van u hebben ontvangen, aan u over te dragen of op uw verzoek aan een andere organisatie over te dragen.
CADANS PRIMAIR zal geen besluiten nemen over uw kind, die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens. Beslissingen worden nooit zonder menselijke tussenkomst genomen.

Als u het niet eens bent met hoe wij omgaan met de gegevens van uw kind, dan kunt u opheldering vragen bij de directeur van uw school. Als u daarna nog vragen heeft, kunt u onze Functionaris voor Gegevensbescherming benaderen: fg@dommelgroep.nl . Indien uw probleem volgens u niet goed wordt opgelost, dan kunt u dat melden bij Autoriteit voor de Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Wijzigingen
CADANS PRIMAIR kan dit document aanpassen, bijvoorbeeld als de verwerking van persoonsgegeven wijzigt. De nieuwe versie zal op de website van onze school worden geplaatst.

Datum laatste wijziging: januari 2019

DOMMELGROEP

Privacyverklaring voor medewerkers

Contactgegevens CADANS PRIMAIR: Schildershof 1a, 5271 BM Sint-Michielsgestel

Contactgegevens Functionaris voor Gegevensbescherming: fg@dommelgroep.nl

Het bestuur verwerkt uw persoonsgegevens. CADANS PRIMAIR is wettelijk verantwoordelijk. CADANS PRIMAIR vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving. We leggen u graag uit hoe het bestuur met uw persoonsgegevens omgaat.

Waarom verwerken wij uw gegevens?
CADANS PRIMAIR verwerkt persoonsgegevens om de verplichtingen als werkgever te kunnen nakomen.
Welke persoonsgegevens wij van u verwerken vindt u hieronder:

Categorie	Toelichting
1. Contactgegevens	1a: naam, voornaam, e-mail, opleiding; 1b: geboortedatum, geslacht; 1c: overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen.
2. werknemersnummer	een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1
3. Nationaliteit en Geboorteplaats	
4. Verzuim en verlof gegevens	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de medewerker, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen geven.
5.Professionalisering	gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: • Diploma's en certificaten • Gevolgde cursussen • Curriculum vitae
6. Financiën	gegevens voor het berekenen, vastleggen en uitbetalen van salaris of vergoedingen (denk hierbij aan een bankrekeningnummer.
7. BSN	Werkgever is verplicht het BSN te gebruiken in hun administratie.

DOMMELGROEP

Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid. CADANS PRIMAIR zal niet meer gegevens verwerken dan noodzakelijk is om de rechten en plichten na te komen. Dit betekent ook dat we de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen.

Welke rechten hebben medewerkers?
Medewerkers kunnen op elk moment gebruik maken van de rechten. Dit betekent bijvoorbeeld dat u altijd een verzoek kunt indienen om inzage te krijgen in de gegevens die wij van u verwerken.

Daarnaast kunt u ook een verzoek indienen om gegevens te rectificeren, te beperken of helemaal te wissen uit het systeem van het bestuur. U heeft altijd het recht om onjuiste gegevens aan te vullen of te verbeteren.

Als u ons verzoekt om uw gegevens beperken of te wissen, zullen wij toetsen of dit mogelijk is.
In deze toets houden wij ons aan de wettelijke voorschriften en kijken wij bijvoorbeeld of wij geen wettelijke plicht hebben om de gegevens te bewaren.
Tevens heeft u het recht om te vragen om de gegevens, die wij van u verwerken en wij van u hebben ontvangen, aan u over te dragen of op uw verzoek aan een andere organisatie over te dragen.

Als u het niet eens bent met hoe wij omgaan met uw gegevens, dan kunt u opheldering vragen bij de leidinggevende. Als u daarna nog vragen heeft, kunt u onze Functionaris voor Gegevensbescherming benaderen: fg@dommelgroep.nl . Indien uw probleem volgens u niet goed wordt opgelost, dan kunt u dat melden bij Autoriteit voor de Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

DOMMELGROEP

Bijlage 2: Rollen en taken

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij de Dommelgroep.

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Richtinggevend (strategisch)	CvB Directeur Contactpersonen AVG	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten • Regelmatig overleg met FG. • Lid van Denktank AVG.	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Functionaris voor Gegevensbescherming	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ICT en internetgebruik

		• Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen • Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Gedragscode medewerkers en leerlingen • Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	ICT-er of applicatie beheerder en medewerker	• Classificatie / risicoanalyse in samenwerking met verantwoordelijke IBP / • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Checklist voor Classificatie- en risicoanalyse. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Uitvoerend (operationeel)	ICT-er of applicatie beheerder en medewerker Directeur	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken
	Contactpersonen AVG	• Informatieverstrekking AVG van FG naar alle scholen	• Uitvoeren afspraken

DOMMELGROEP

Bijlage 3: Functiebeschrijving FG

Functionaris Gegevensbescherming Dommelgroep

Context

Dommelgroep is een coöperatieve vereniging bestaande uit vijf stichtingen die primair onderwijs verzorgen. Onder de Dommelgroep vallen in totaal 42 basisscholen, met ongeveer 850 personeelsleden en 10.000 leerlingen. De Dommelgroep bestrijkt het gebied in de Meierij dat gelegen is tussen de stedelijke gebieden met aan het noorden 's-Hertogenbosch en in het zuiden Eindhoven/ Son en Breugel.
De Dommelgroep heeft een shared servicecentrum dat diensten levert op het gebied van personeelszaken, financiën en huisvesting. Daarnaast heeft de Dommelgroep conform het bepaalde in de privacywet, de 'Algemene Verordening Gegevensverwerking' een functionaris Gegevensbescherming aangesteld.
De Dommelgroep streeft naar optimale informatiebeveiliging en bescherming van privacy en heeft daartoe een informatiebeveiligings- en privacybeleid opgesteld. De Functionaris gegevensbescherming (hierna te noemen FG) opereert zelfstandig, is onafhankelijk en houdt toezicht op de toepassing en naleving van privacywetgeving conform de 'Algemene Verordening Gegevensverwerking'.

De FG is verantwoordelijk voor het toezicht op de uitvoering van het vastgestelde beleid op het terrein van informatiebeveiliging en privacy en doet voorstellen voor mogelijke verbeteringen op dit terrein. De FG stelt rapportages op met betrekking tot de stand van zaken van de informatiebeveiliging. De FG adviseert en rapporteert aan de bestuurders van de stichtingen.

Resultaatgebieden

Bijdragen aan ontwikkeling van informatiebeveiliging

- Signaleert en rapporteert over de stand van zaken m.b.t. de naleving van de AVG in onderdelen van de instelling aan de betreffende directeur portefeuillehouder Informatiebeveiliging en Privacy (IBP) binnen het bestuur;
- Indien er niet gehandeld wordt naar voorgenoemde voorschriften en regelingen, dit bespreekbaar maken en vervolgens afspraken maken met de verantwoordelijke functionaris.
- Adviseert en ondersteunt onderdelen van de onderwijsinstelling bij de verbetering en evaluaties m.b.t. naleving van de AVG (verloop, inhoud en resultaat) en werkt daarbij planmatig (conform PDCA-cyclus).
- Anticipeert op ontwikkelingen binnen een tijdshorizon van maximaal 2 tot 3 jaar;

Uitvoering wet Algemene Verordening Gegevensbescherming (AVG)

- Houdt toezicht op, rapporteert over en adviseert over de verwerking van persoonsgegevens binnen alle onderdelen van de organisatie;

- Levert een bijdrage aan het ontwerpen en evalueren van procedures, planningen en instrumenten met betrekking tot de AVG;
- Doet onderzoek naar de naleving van de AVG en het bewaken ervan;
- Leidt of neemt deel aan overlegvormen, projecten en samenwerkingsverbanden op het gebied van de informatiebeveiliging en privacy;

- Fungeert als aanspreekpunt voor zaken betreffende de AVG binnen de onderwijsinstelling;
- Levert een bijdrage aan interne en externe rapportages en verantwoordingsdocumenten op het terrein van informatiebeveiliging en privacy;
- Draagt zorg voor de toepassing van de AVG en zorgt voor een passend niveau van beveiliging van de informatiehuishouding;
- Neemt maatregelen gericht op het beperken van (het gebruik van) persoonsgegevens.
- Houdt een bestand van verwerkingen van persoonsgegevens (dataregister) bij;
- Behandelt vragen en klachten m.b.t. de AVG;
- Geeft voorlichting over het gebruik van persoonsgegevens en bevordert awareness bij medewerkers rondom hun verplichtingen bij het verwerken van persoonsgegevens d.m.v nieuwsbrieven en workshops;
- Treedt op als intermediair tussen de onderwijsinstelling en de Autoriteit Persoonsgegevens;
- Neemt deel aan overleg over de uitvoering van het IBP-beleid.

Control

- Levert een bijdrage aan de kwaliteit van het niveau van informatiebeveiliging binnen de instelling;
- Levert een bijdrage aan en adviseert over (het initiëren van) informatiebeveiliging- assessments -tests, -reviews en –audits uit;
- Levert een bijdrage aan interne en externe jaarrapportages en verantwoordingsdocumenten over het niveau van de informatiebeveiliging;
- Informeert de portefeuillehouder IBP m.b.t de naleving van de eisen m.b.t de AVG.

Kader, verantwoordelijkheden en bevoegdheden

Beslist over: de rapportages, interne en externe verantwoordingsdocumenten m.b.t. de naleving van de AVG en adviezen over de verwerking van persoonsgegevens binnen alle onderdelen van de organisatie.

Kader: De AVG en afgeleide wet- en regelgeving, onderwijswetgeving, kwaliteitsstandaarden, richtlijnen en specifiek geformuleerde beleidslijnen ten aanzien van informatiebeveiliging en privacy.

Verantwoording: de portefeuillehouder IBP binnen CADANS PRIMAIR over de kwaliteit van de rapportages m.b.t. de naleving van de AVG, de afspraken met de verantwoordelijke functionaris, de bijdrage aan het ontwerpen, bewaken en evalueren van procedures, planningen en instrumenten en het onderzoek naar de naleving van de AVG.

DOMMELGROEP

Contacten

- Met bestuurder(s) en directeuren (proceseigenaren) van de onderwijsinstelling om met uiteenlopende belangen om te gaan, informatie te geven en de uitvoering af te stemmen;
- Met directeuren (proceseigenaren) van de onderwijsinstelling om informatie te geven en de naleving van de AVG af te stemmen;
- Met directies en medewerkers over de toepassing van richtlijnen, procedures, processen en werkwijzen voor het gebruik van bestaande, aangepaste of nieuwe voorzieningen, methoden en/of technieken op het terrein van informatiebeveiliging om hen te informeren, vragen te beantwoorden;
- Met de portefeuillehouder IBP over de wijze waarop de werkzaamheden dienen te worden uitgevoerd, de evaluatie van de resultaten daarvan, verbetervoorstellen en om informatie uit te wisselen en tot afstemming te komen.
- Met de AVG ‘Denktank’.

DOMMELGROEP

Bijlage 4: Protocol ICT en Social media voor leerlingen

Algemeen

We behandelen elkaar met respect en laten iedereen in zijn waarde.
Iedereen is verantwoordelijk voor wat hij/zij zelf plaatst op sociale media en kan daarop aangesproken worden.
We helpen elkaar om goed en verstandig met internet en sociale media om te gaan en we spreken elkaar ook daar op aan.
Denk altijd na voordat je iets verstuurt.

Internet en e-mail

We vinden het van groot belang dat je als leerling zo veilig mogelijk online kan werken. Om hiervoor te zorgen, zijn de volgende gedragsregels van belang:

1. Ik gebruik het internet om informatie te zoeken over een onderwerp of werkstuk voor school. Ik bezoek geen sites die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn.
2. Ik vraag toestemming van mijn juf of meester, als ik…

a. een online game wil spelen
b. persoonlijke gegevens (naam, adres en je telefoonnummer) moet invullen op een website
c. bestanden wil downloaden of delen
d. een e-mail wil versturen
e. mijn mobiele telefoon wil gebruiken

3. Wees zuinig met je e-mailadres. Je e-mailadres is geld waard! Laat deze dus niet zomaar overal achter.
4. Ik deel geen wachtwoorden met anderen.
5. Ik ga voorzichtig om met mails die ik niet vertrouw of waarvan ik de afzender niet ken. Bij twijfel klik ik geen linkjes aan.
6. Ik vertel direct aan mijn meester of juf als ik informatie tegenkom die ik niet prettig vind of waarvan ik weet dat dat niet hoort.
7. Ik weet bij welke instanties/personen ik op school en buiten school terecht kan als ik iets onprettigs heb meegemaakt op het internet waarbij ik me niet veilig voel.
8. Ik bekijk informatie op internet kritisch en kan beoordelen of het echt of nep is.
9. Ik ken de gevolgen van het delen van informatie die niet echt is.

Sociale media

Binnen de school gelden de volgende gedragsregels om te zorgen dat de mogelijkheden van sociale media worden gebruikt zonder andere personen of de school te schaden:

10. Ik plaats geen foto’s of verhalen over een ander (leerling, juf of meester, school, ouders of anderen van buiten de school) op sociale media als een ander dit niet goed vindt.

11. Ik plaats geen kwetsende foto's, verhalen of opmerkingen op sociale media. Ook gebruik ik geen grove taal.
12. Ik doe niet mee aan pesten via de Whats app. Als ik nare berichten ontvang van iemand, dan vertel ik dit op school of thuis.
13. Als ik iemand niet begrijp via de Whats app of andere berichten, dan vraag ik dit rechtstreeks aan diegene.
14. Ik ga zorgvuldig om met mijn eigen identiteit. Ik besef dat ik altijd terug te vinden ben op internet.

ICT-apparatuur

De ICT-apparatuur op school (laptop, tablet, 3d-printer, digibord, scanner, etc.) is niet goedkoop, daarom dien je hier voorzichtig mee om te gaan. De volgende gedragsregels zijn daarom van belang:

15. Ik gebruik alleen ICT-apparatuur en software waar ik toestemming voor heb gekregen van de meester of juf. Dat geldt ook voor meegebracht smartphones, etc.
16. Ik ga voorzichtig om met de dure ICT-apparatuur van de school die ik mag gebruiken.
17. Ik gebruik geen meegebrachte USB-sticks van thuis in ICT-apparatuur van de school.

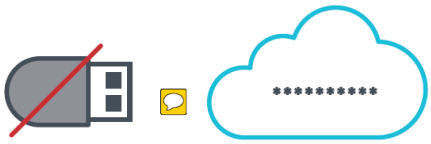
Schermtijd

18. Ik ben me bewust van de wereld buiten de online wereld en ik houd de tijd in de gaten als ik achter de computer / laptop of tablet zit.

DOMMELGROEP

Bijlage 5: Handreiking AVG medewerkers

Hoe bewaar ik bestanden?



Memorysticks raden we af omdat ze snel kwijt kunnen raken. Gebruik voor privacygevoelig materiaal een schijf of cloudservice die beveiligd is met een wachtwoord.

Kan iemand meekijken?

Als er privacygevoelig materiaal op je computer staat, sluit dan altijd je account af, ook wanneer je 'even' wegloopt.

Ben ik de enige die in mijn account kan?

Gebruik alleen je eigen account, dan weet je zeker dat je niet meer ziet dan nodig is voor jouw werkzaamheden. Let ook op dat leerlingen je wachtwoord niet kennen. Surf bewust en controleer of een website een groen slotje heeft.

Is mijn wachtwoord sterk genoeg?

Bedenk een lang, sterk wachtwoord met kleine letters, hoofdletters, cijfers en liefst een die je niet ook ergens anders voor gebruikt. Naam123 en geboortedata vermijden!

Heb ik toestemming?

Weet waar gegevens van leerlingen voor gebruikt mogen worden en met wie je die wel en niet mag delen. Lijstjes met adressen op het prikbord, dat mag niet meer.

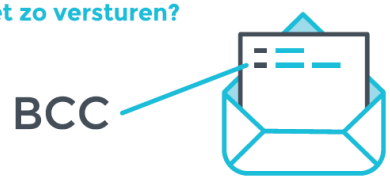
Wat doen we met sociale media?

Spreek af met collega's, ouders en leerlingen wat je plaatst, waar en waarom. Bespreek educatieve en sociale waarden.

Mag ik die foto of video delen?

Bedenk bij iedere foto/video waar leerlingen op voorkomen of er een bezwaar zou kunnen ontstaan als je deze deelt. Jonger dan 16 jaar moeten de ouders toestemming geven. Bij twijfel, raadpleeg de betrokkenen en/of collega's. Deel zo mogelijk via kanalen die aan de AVG voldoen.

Kan ik het zo versturen?



Check of je e-mails BCC verstuurt en dat je alleen privacy-gevoelige informatie deelt via veilige kanalen. Bespreek dit in het team en maak elkaar hiervan bewust. Deel bestanden via AVG-veilige onlinepakketten, liever niet per email.

Is het veilig opgeborgen?

Sluit archiefkasten of ruimtes waar privacygevoelige informatie ligt. Op het kopieerapparaat of in de printerlade blijven soms documenten liggen. Voorkom dat en pak het direct. Vind je zulke informatie? Ga er integer mee om.

Wie is de FG?

Weet wie is aangesteld als Functionaris Gegevensbescherming en meld datalekken zodat hij/zij ze binnen 72 uur bij de Autoriteit Persoonsgegevens kan melden.

DOMMELGROEP

Bijlage 6: Protocol beveiligingsincidenten en datalekken

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het privacy beleid van CADANS PRIMAIR.
Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van CADANS PRIMAIR en al haar medewerkers.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor 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.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht 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. 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. Er is persoonlijke informatie ‘gelekt’. Dit kan zijn een hack, het verliezen van een usb-stick of de diefstal van een laptop. Maar ook een verkeerd verzonden email of een verkeerd ingestelde autorisatie.
De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus CADANS PRIMAIR.
Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

DOMMELGROEP

Afspraken met scholen en leveranciers

CADANS PRIMAIR maakt als verantwoordelijke voor de persoonsgegevens de onderstaande datalek-afspraken met de scholen en de leveranciers die persoonsgegevens ontvangen en verwerken:

- De ontdekker van een datalek meldt dit binnen 24 uur bij de directeur van de school of de zaakgelastigde of contactpersoon van een leverancier.
- De directeur of de zaakgelastigde of contactpersoon meldt binnen 24 uur het datalek bij de Functionaris Gegevensbescherming, bij voorkeur fg@dommelgroep.nl.
- De FG neemt de melding op in het Register Datalekken en doet, na een positieve weging, de melding bij de Autoriteit Persoonsgegevens. Ook informeert hij de bestuurder bij een ernstige datalek.

CADANS PRIMAIR heeft schriftelijke afspraken met verwerkers over datalekken gemaakt d.m.v. de model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Werkwijze

De vier rollen

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

1. **Ontdekker (medewerker of leerling)**; degene die het beveiligingsincident of datalek op het spoor komt.
2. **Meldpunt (directeur)**; een aanspreekpunt per school waar alle beveiligingsincidenten worden gemeld.
3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens en een incidentenregister bijhoudt.
4. **Technicus**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De 7 stappen

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 dit bij de eigen directeur van de school of de zaakgelastigde of contactpersoon van een leverancier van de school.

2. **Inventariseren**

De directeur zal samen met de melder de vragenlijst in de bijlage zo compleet mogelijk invullen.

3. Beoordelen

Wanneer de vragenlijst is ingevuld, stuurt de directeur - nog op dezelfde dag van de ontdekking- het formulier naar de FG - fg@dommelgroep.nl - met het verzoek het datalek te beoordelen.

De FG informeert na ontvangst van het meldingsformulier direct de bestuurder.

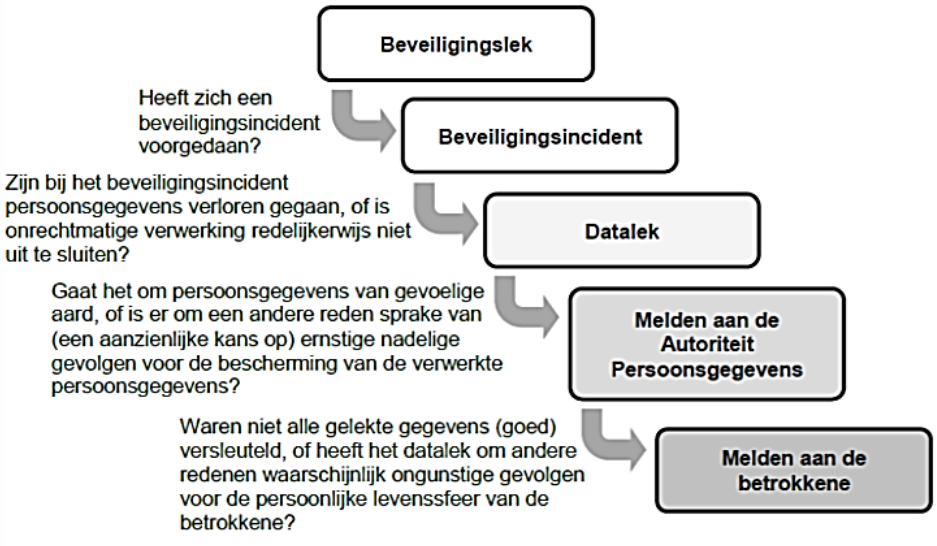
De FG beoordeelt de informatie om te bepalen of ook een melding aan de Autoriteit persoonsgegevens vereist is en informeert de bestuurder over zijn conclusie.

De volgende informatie over het datalek wordt vastgelegd door de FG:

- De feiten rondom het datalek, de mogelijke gevolgen van het datalek en het ingevulde meldingsformulier.
- Is het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- De inhoud van de melding.
- Is het datalek gemeld aan de betrokkenen? Waarom niet?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', houdt de FG rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen wordt er gemeld bij de Autoriteit Persoonsgegevens.

De onderstaande beslisboom wordt gebruikt:



4. Beperken gevolgen

De gevolgen worden zoveel mogelijk beperkt. Er wordt gekeken wat de oorzaak van het beveiligingsincident is. De nodige acties voor de aanpak en het verhelpen van de oorzaak worden uitgevoerd.

5. **Melden**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens, dan zal de FG dit binnen een werkdag 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/actionpage?0.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de FG waarmee het incident is afgesloten. De FG informeert de directeur van de school over de genomen (te nemen) maatregelen om herhaling te voorkomen.

7. **Informeren betrokkene: leerling en/of zijn ouders**
   Wanneer het datalek waarschijnlijk een hoog risico inhoudt voor de betrokkene(n), dan wordt het datalek ook aan de betrokkene(n) zelf gemeld. Dat zijn medewerkers, leerlingen, of hun ouders als zij jonger zijn dan 16 jaar.

   In principe wordt ervan uitgegaan dat het lekken van persoonsgegevens van kinderen altijd van gevoelige aard is en gemeld moet worden bij de betrokkenen.
   Als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn volledig onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld.

Monitoring beveiligingsincidenten en datalekken

De FG maakt jaarlijks een analyse van de meldingen van de beveiligingsincidenten en de datalekken. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.
De bestuurder wordt door de FG geïnformeerd over de uitkomsten van de analyse.

DOMMELGROEP

Meldingsformulier beveiligingsincident / datalek (invullen en insturen door directeur)

Dit formulier invullen en insturen door directeur van de school naar: fg@dommelgroep.nl

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **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.

1 Datum/periode van het beveiligingsincident / datalek.
2 Gegevens van de melder (naam, functie, hoe te bereiken).
3 Gegevens stichting en school.
Naam stichting: Registratienummer Kamer van Koophandel: Naam school: Naam, e-mail en telefoonnummer directeur:
4 Toedracht van het incident.
5 Korte beschrijving van het incident (bijv. verlies, diefstal).
6 Wat voor soort gegevens zijn er bij het incident betrokken (welke persoonsgegevens)?
7 Wie is er verantwoordelijk voor het datalek (welke persoon of organisatie)?
8 Welke actie is al ondernomen?

DOMMELGROEP

Bijlage 7: Jaarlijks Toestemmingsformulier gebruik beeldmateriaal

Beste ouder/verzorger,

Op onze school laten wij u met beeldmateriaal zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en lessen. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn.
Natuurlijk gaan we zorgvuldig om met het beeldmateriaal. We plaatsen bij het beeldmateriaal geen namen van leerlingen.

Met dit formulier vragen we uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Wilt u de antwoordstrook met uw kind meegeven en afgeven aan de leerkracht? Per kind een apart formulier invullen a.u.b..

Deze toestemming geldt alleen voor foto's en video's die door ons, of in onze opdracht worden gemaakt. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten. De school heeft daar geen invloed op en is daar niet voor verantwoordelijk.
Daarnaast vragen wij uw toestemming voor het delen van de klassenfoto met klasgenoten.
Wilt u uw toestemming samen met uw zoon/dochter bespreken? We merken dat oudere leerlingen soms zelf een keuze willen maken om foto's te gebruiken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van beeldmateriaal wel of niet mag.
Als we beeldmateriaal voor een ander doel willen gebruiken, vragen we u apart om toestemming.
U mag natuurlijk altijd uw toestemming weer intrekken. Geef dit dan door aan de directeur.
Alvast bedankt voor uw medewerking!

Met vriendelijke groet,

Naam directeur

Hierbij geeft ondergetekende, ouder / verzorger van …….. groep ……..

1. wel /geen* toestemming dat basisschool
   klassenfoto's maakt die met klasgenoten gedeeld worden (*doorhalen wat van toepassing is)
2. Toestemming voor gebruik beeldmateriaal**
   (** hieronder aankruisen waarvoor u toestemming geeft)

☐ in de schoolgids
☐ in oudercommunicatietool (app/website)
☐ in nieuwsbrieven
☐ op de website van school
☐ op sociale media
☐ in persberichten door school aangeleverd

Datum: ……
Naam ouder/verzorger: ……
Handtekening ouder/verzorger: ……

DOMMELGROEP

Bijlage 8: Eenmalige toestemming adresgegevens, telefoonnr, e-mailadres

Beste ouder/verzorger,

Met dit formulier vragen we uw toestemming voor het gebruik van adres, telefoon en e-mailadres van uw zoon/dochter. Wij verzoeken u onderstaande gegevens in te vullen en in te leveren bij de directeur van de school.

Met vriendelijke groet,

…….directeur

Eenmalige toestemming adres, telefoon en e-mailadres:

Hierbij verklaart ondergetekende, ouder / verzorger van:			
Naam leerling :		Groep:	
Naam leerling:		Groep:	
Naam leerling:		Groep:	
Naam leerling:		Groep:	

- Dat de adreslijst met de naam van mijn kind, adres en telefoonnummer verspreid mag worden in de klas van mijn kind. ☐ JA ☐ NEE
- Dat het emailadres van de ouder/verzorger verspreid mag worden in de klas van mijn kind. ☐ JA ☐ NEE
- Dat de adreslijst, het telefoonnummer en e-mailadres gebruikt mogen worden voor het verstrekken van schoolspecifieke informatie en onderwijsdoeleinden ☐ JA ☐ NEE

- *A.u.b. aankruisen waarvoor u toestemming geeft*

Datum: .....

Naam ouder/verzorger: .....

Handtekeningen ouder(s)/verzorger(s): .....

.....

DOMMELGROEP

Bijlage 9: Geheimhoudingsverklaring

Geheimhoudingsverklaring

Beleid en maatregelen zijn niet voldoende om persoonsgegevens passend te beschermen. De feitelijke omgang met persoonsgegevens door alle medewerkers die werkzaam zijn voor één van de besturen van de Dommelgroep dient zorgvuldig te zijn en in overeenstemming met de AVG. Dat betekent dat al deze personen de persoonsgegevens die zij verwerken, geheim dienen te houden. Dit wordt geregeld d.m.v. deze geheimhoudingsverklaring.

Ondergetekende:
Naam:

Rol/ functie binnen Cadans Primair:

Organisatieonderdeel / school:

Hierna te noemen: werknemer

Overwegende:

dat werknemer voor de uitvoering van zijn of haar functie de beschikking moet hebben over informatie en/of persoonsgegevens, door Cadans Primair verzameld in haar hoedanigheid als verantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming;

dat Cadans Primair wil benadrukken dat zij de zorgvuldige omgang met deze gegevens van groot belang vindt en daarom voorwaarden stelt aan het ter beschikking stellen van deze gegevens aan werknemer;

dat Cadans Primair tevens moet voldoen aan haar wettelijke verplichting tot het treffen van technische en organisatorische beveiligingsmaatregelen ten aanzien van deze informatie en/of persoonsgegevens.

dat werknemer door het ondertekenen van deze verklaring erkent dat Cadans Primair deze informatie en/of persoonsgegevens als geheim en vertrouwelijk beschouwt en dat werknemer schade kan berokkenen door onzorgvuldige omgang met en/of het onrechtmatig aan derden ter beschikking stellen van deze informatie.

DOMMELGROEP

verklaart dat:

de werknemer de informatie en/of persoonsgegevens alleen zal gebruiken voor de duur van het dienstverband en uitsluitend voor de werkzaamheden binnen de functie van de werknemer;

de werknemer de informatie en/of persoonsgegevens niet zonder voorafgaande toestemming van Cadans Primair verstrekt aan derden;

de werknemer uiterste zorg besteedt aan een deugdelijke en veilige opslag van de informatie en/of persoonsgegevens, ter voorkoming van verlies en/of enige vorm van onrechtmatige verwerking, en hiertoe de richtlijnen en instructies opvolgt die de Cadans Primair verstrekt en voorschrijft;

het voorgaande geldt ook voor door of namens Cadans Primair verstrekte toegang aan werknemer tot ICT-systemen en/of ter beschikking gestelde apparatuur;

de werknemer zich verplicht alle door of namens Cadans Primair verstrekte informatie en/of persoonsgegevens te retourneren aan Cadans Primair, zodra daarom verzocht wordt. De werknemer zal geen kopieën van de informatie bewaren;

de werknemer erkent dat Cadans Primair altijd rechthebbende en eigenaar blijft van de verstrekte informatie en/of persoonsgegevens;

de afspraken in deze verklaring ook na beëindiging van het dienstverband geldig blijven.

Ondertekening:

plaats:

datum:

naam:

handtekening:

DOMMELGROEP

Bijlage 10: IBP bij Leerlingdossiers en onderwijskundige rapporten (zoals bij OSO en LDOS)

Leerlingdossiers

- U mag alleen gegevens verwerken in het leerlingdossier voor zover dat noodzakelijk is voor het doel.
- De gegevens die u verwerkt in het leerlingdossier, moeten juist zijn.
- U regelt de beveiliging van en de toegang tot de leerlingdossiers goed.
- U kunt aantonen dat u bij het gebruik van leerlingdossiers de regels van de AVG naleeft. Dit heet de verantwoordingsplicht.
- U neemt de gegevensverwerking in leerlingdossiers op in uw register van verwerkingsactiviteiten.
- U kunt verplicht zijn om een data protection impact assessment (DPIA) uit te voeren voor uw gebruik van het leerlingdossier.
- Houd er rekening mee dat ouders en/of leerlingen het recht op dataportabiliteit hebben. Dat is het recht om gegevens mee te nemen. Bijvoorbeeld naar een andere school.

Onderwijskundig rapport

Een basisschool mag alleen gegevens over een leerling in het onderwijskundig rapport opnemen die in de volgende categorieën vallen:

- administratieve gegevens (zoals naam, adres en onderwijsnummer van de leerling);
- gegevens over onderwijshistorie en leerresultaten (zoals een eventuele overstap tussen scholen en toetsresultaten);
- gegevens over de sociaal-emotionele ontwikkeling en het gedrag van het kind (zoals het gedrag in de omgang en zijn/haar werkhouding);
- gegevens over de eventuele extra begeleiding die het kind heeft gekregen of nodig heeft;
- gegevens over de verzuimhistorie (ongeoorloofd verzuim van het kind in het jaar voorafgaand aan het onderwijskundig rapport).

DOMMELGROEP

Bijlage 11: Overzicht bewaartermijnen

Bewaartermijn leerlinggegevens

- In het lager en voortgezet onderwijs geldt dat u gegevens over verzuim en afwezigheid en in- en uitschrijving 7 jaar moet bewaren nadat de leerling is uitgeschreven.
- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen, moet u als school 7 jaar na het vertrek van de leerling bewaren.
  Een school mag adresgegevens van oud-leerlingen bewaren voor het organiseren van reünies. Let er wel op dat hiervoor eerst toestemming gevraagd wordt aan de oud-leerlingen. Deze gegevens mogen alleen voor dat doel gebruikt worden.

Hoe lang mag een stichting het personeelsdossier bewaren?

De bewaartermijnen van personeelsgegevens zijn afhankelijk van verschillende wetgeving.
Sollicitatiegegevens
Deze informatie (sollicitatiebrief, cv., gespreksaantekeningen) wordt uiterlijk na 4 weken vernietigd tenzij met de sollicitant anders is overeengekomen. Een assessment of psychologisch onderzoek kan deel uitmaken van de procedure. Ook deze gegevens worden uiterlijk na vier weken, nadat de procedure is beëindigd, vernietigd, met uitzondering van de gegevens van degene die in dienst genomen wordt.
Personeelsgegevens
Over het algemeen geldt voor personeelsgegevens een bewaartermijn van twee jaar nadat het dienstverband is beëindigd. Mochten die gegevens echter in een eerdere fase al niet meer nodig zijn, dan moeten ze direct verwijderd worden.
Gegevens van (ex-)werknemers kunnen langer bewaard worden indien er een arbeidsconflict met deze persoon is (geweest) of als er een rechtszaak loopt. Tevens mogen gegevens langer bewaard worden als een (ex-)werknemer hiervoor toestemming heeft gegeven. Geadviseerd wordt om gegevens van ex-medewerkers, die nog moet bewaard worden, van het actieve bestand naar een passief bestand te verplaatsen.
In tegenstelling tot de archiefwet is de belastingwetgeving wel van toepassing. Voor gegevens uit de salarisadministratie die fiscaal van belang zijn, bestaat een bewaarplicht van zeven jaar na het einde van de dienstbetrekking. Daarnaast moeten loonbelastingverklaringen en kopieën van een identiteitsbewijs tot vijf jaar na het einde van de dienstbetrekking bewaard worden.

Vernietiging of archiefbestemming
Als persoonsgegevens niet meer nodig zijn of de bewaartermijn is verlopen, dan moeten die gegevens verwijderd worden. Verwijderen betekent niet dat de gegevens vernietigd moeten worden.

Het is voldoende de gegevens buiten het bereik van de actieve administratie te brengen en in een archief of op een aparte schijf op te slaan.
De Dommelgroep mag, op vrijwillige basis, persoonsgegevens in een archief bewaren dat bestemd is voor historische, statistische of wetenschappelijke doeleinden mits hierbij voldaan wordt aan de eisen m.b.t. bescherming van deze gegevens volgens de AVG.
Voor de wijze waarop gegevens vernietigd moeten worden, bestaat geen harde regel. Men moet zorgvuldig met de vernietiging van gegevens omgaan. De gevoeligheid van persoonsgegevens (leerling of medewerker) is groot. Met het oog hierop is een oud-papierbak niet de juiste plaats om deze gegevens in af te voeren. Een papierversnipperaar of een in papierafvoer gespecialiseerd bedrijf is de aangewezen weg. Voor digitaal opgeslagen gegevens zijn systemen beschikbaar die automatisch gegevens vernietigen op een van tevoren aangegeven tijdstip.