Scholengroep Over- en Midden-Betuwe

Privacyreglement

VO - PO

Versie 19-11-2019

Basis	
Wet en regelgeving	**Algemene Verordening Gegevensverwerking (AVG)**
Archief CvB	**PZ 0.8**
Van toepassing op/voor	**Gehele scholengroep Over- en Midden-Betuwe**

Status	**Data**	**Opmerkingen**
Concept (versie/datum)	**1/15-11-18** **2/29-01-19** **3/juni 2019** **4/19-11-19**	**2/Toevoeging medewerker kwaliteitszorg in bijlage I-A** **3/wijziging bijlage VI** **4/Red. aanpassing adres functionaris gegevensbescherming**
Goedkeuring (dir. / CvB / CvB)	**13-12-2018**	**Bespreken DO**
Inspraak (advies/instemming PGMR)	**31-01-2019**	**VO:** **Instemming PGMR cf. artikel 31 lid 1 sub m en sub n, GMR-reglement.** **Instemming ouderdeel cf. artikel 32 lid b, GMR-reglement.** **Instemming leerlingendeel cf. artikel 33 lid b, GMR-reglement.**
	14-01-2019	**PO:** **Instemming PMR cf. artikel 29 lid 1 sub m en sub n, MR-reglement LvB.** **Instemming ouderdeel cf. artikel 30 lid , MR-reglement LvB.**
Vastgesteld (door/datum)	**CvB / 01-02-2019**	
in werking op (datum)	**01-02-2019**	

Missie en visie

De Scholengroep Over- en Midden-Betuwe is er voor de leerlingen in de regio. Zij biedt ambitieus onderwijs dat eisen stelt en waar ieders talent (h)erkend wordt. De scholengroep neemt een zichtbare plek in binnen de samenleving en biedt leerlingen en medewerkers veiligheid. Zo wil de scholengroep de leerlingen eigentijds en wereldwijs onderwijs aanbieden. Vanuit een solide basis biedt de scholengroep een uitdagende en dynamische leeromgeving.

Wij bieden onze leerlingen een veilige leeromgeving en onze medewerkers een veilige werkplek. Een goede en zorgvuldige omgang met persoonsgegevens binnen de school is daarvoor een randvoorwaarde.

De Algemene Verordening Gegevensbescherming (AVG) stelt nieuwe en verdergaande eisen aan de omgang met persoonsgegevens. Het privacyreglement van de Stichting Christelijk Onderwijs Over- en Midden-Betuwe en het beleid dat daaraan ten grondslag ligt hebben wij daarom herzien en aangevuld op de punten waar de AVG dit vereist.

Met het reglement beoogt de Stichting Christelijk Onderwijs Over- en Midden-Betuwe ervoor zorg te dragen dat op haar scholen de verwerking van persoonsgegevens plaatsvindt conform de Verordening, de implementatiewet Verordening, sectorgedragscodes, sectorbeveiligingscodes en organisatie-specifieke (interne) regelingen.

Dit houdt onder andere in dat:

a. de persoonlijke levenssfeer van betrokkene wordt beschermd tegen onrechtmatige verwerking en/of misbruik van die gegevens, tegen verlies en tegen het verwerken van onjuiste gegevens;
b. wordt voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn; en
c. de verwerkingen niet leiden tot een hoog risico voor de betrokkenen.

Het college van bestuur zal in samenspraak met de functionaris gegevensbescherming passende maatregelen ten uitvoer leggen en verantwoording afleggen over het gevoerde beleid aan de ouder- en personeelsgeleding van de medezeggenschapsraad en aan de Raad van Toezicht.

College van bestuur

Inhoudsopgave

Artikel 1. Begripsbepalingen

Voor de toepassing van dit reglement en de daarbij behorende bijlagen wordt verstaan onder:

a. *Algemene Verordening Gegevensbescherming (AVG)*: de Verordening;

b. *Autoriteit Persoonsgegevens*: toezichthoudende autoriteit, als bedoeld in artikel 51 van de AVG (hierna ook AP);

c. *bestand*: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

d. *betrokkene*: degene op wie een persoonsgegeven betrekking heeft (een sollicitant, een medewerker werkzaam/werkzaam geweest bij de Stichting Christelijk Onderwijs Over- en Midden-Betuwe, een leerling ingeschreven/ingeschreven geweest aan een school behorende tot de Stichting of een ouder/verzorger van wie gegevens in de persoonsregistratie zijn opgenomen, alle overige personen werkzaam bij of ten dienste van de Stichting, waaronder de leden van het toezichthoudend orgaan, leveranciers en dienstverleners, huurders en tenslotte de bezoekers van één van de schoolgebouwen van de Stichting);

e. *derde*: degene, niet zijnde de verwerker of degene die onder gezag van de verwerkingsverantwoordelijke werkzaam zijn, die door de verwerker gemachtigd is om persoonsgegevens te verwerken;

f. *dienst van de informatiemaatschappij*: dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht;

g. *gegevensbeschermingseffectbeoordeling*: een beoordeling van het effect van de beoogde verwerking op de bescherming van persoonsgegevens;

h. *groep*: een economische eenheid waarin rechtspersonen organisatorisch verbonden zijn (artikel 2:24 BW);

i. *leerling*: persoon die onderwijs volgt of gaat volgen op een school van de Stichting;

j. *leerling- of personeelsnummer*: eenduidig nummer dat wordt gebruikt ten behoeve van efficiënte verwerking van persoonsgegevens;

k. *personeel*:

   a. de bij de Stichting werkzame directeur, (adjunct-)directeur, afdelingsleider/directielid of leraar, en overige medewerkers benoemd/aangesteld in een andere functie dan het geven van onderwijs, waaronder begrepen de leden van het bestuur van die scholen die zijn benoemd door een raad van toezicht als bedoeld in artikel 17c, vierde lid van de WPO, respectievelijk artikel 24e1, vierde lid van de WVO, voor zover die leden mede zijn benoemd op basis van een arbeidsovereenkomst/aangesteld op een akte;

   b. de onder a bedoelde medewerker die zonder benoeming/aanstelling is tewerkgesteld bij of ingeleend door de Stichting;

m. *persoonsgegevens*: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’);

n. *pseudonimisering*: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan de specifieke persoon kunnen worden gekoppeld, zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

o. *school*: een basisschool of school voor voortgezet onderwijs als bedoeld in respectievelijk artikel 1 van de WPO en artikel 1 van de WVO die in stand wordt gehouden door de Stichting;

p. *schoolbegeleiding*: activiteiten ten behoeve van de schoolorganisatie of het onderwijs aan een school die dienen tot begeleiding, ontwikkeling, advisering, informatieverstrekking en evaluatie, alsmede activiteiten tot bevordering van een optimale schoolloopbaan van leerlingen;

q. *Stichting:* Stichting Christelijk Onderwijs Over- en Midden-Betuwe;

r. *toestemming van betrokkene*: elke vrije, specifieke, geïnformeerde ondubbelzinnige wilsuiting door middel van een verklaring of een ondubbelzinnig actieve handeling, waarmee betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt;

s. *het toezichthoudend orgaan*: de Raad van Toezicht of de toezichthoudende bestuurder ingeval er geen Raad van Toezicht is;

t. *Verordening:* Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;

u. *verwerking van persoonsgegevens*: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen of vernietigen van gegevens;

v. *verwerkingsverantwoordelijke*: de Stichting;

w. *verwerker*: degene die op basis van een overeenkomst ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

x. *WPO*: Wet op het primair onderwijs;

y. *WVO:* Wet op het voortgezet onderwijs. Voor scholen welke zowel primair als voortgezet onderwijs aanbieden, wordt in dit reglement gelijke toepassing gegeven aan de gelijkluidende wetsbepalingen in de wetgeving ten aanzien van het primaire onderwijs;

z. *Functionaris gegevensbescherming (FG):* interne toezichthouder op de verwerking van persoonsgegevens binnen een organisatie;

aa. *IRT:* het Incident Response Team van de scholengroep.

Artikel 2. Verantwoordelijkheden

2.1. De Stichting is verantwoordelijk voor:

a. een rechtmatige, behoorlijke en transparante gegevensverwerking;

b. het vaststellen van welbepaalde duidelijk omschreven en gerechtvaardigde doeleinden alsmede een verwerking conform de vastgestelde doeleinden;

c. een minimale gegevensverwerking, dat wil zeggen dat het gebruik van gegevens wordt beperkt tot hetgeen noodzakelijk is voor de doeleinden waarvoor deze worden verwerkt;

d. het gebruik van juiste en geactualiseerde gegevens en het wissen respectievelijk corrigeren van gegevens die onjuist zijn;

e. opslagbeperking van gegevens, dat wil zeggen dat deze niet langer worden bewaard dan nodig voor de vastgestelde doeleinden;

f. het nemen van passende technische en organisatorische maatregelen;

2.2. De Stichting laat zich bij bovengenoemde taken adviseren door de functionaris gegevensbescherming.

Beleidskader

2.1.a.

- Reglement
- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Brondocumenten/ brongegevens en bewaartermijnen (bijlage I-B)
- Privacyverklaring (bijlage VIII)

2.1.b.

- Reglement
- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Brondocumenten/ brongegevens en bewaartermijnen (bijlage I-B)

2.1.c.

- Reglement
- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Brondocumenten/ brongegevens en bewaartermijnen (bijlage I-B)

2.1.d.

- Toestemmingsformulier oud-personeelsleden (bijlage V-A)
- Toestemmingsformulier oud-leerlingen (bijlage V-B)

2.1.e.

- Brondocumenten/ brongegevens en bewaartermijnen (bijlage I-B)

2.1.f.

- Protocol gebruik van e-mail, ICT en sociale media (bijlage II)
- Protocol gebruik van camera- en videobeelden (bijlage III)
- Geheimhoudingsverklaring (bijlage IV)
- Handboek datalekken (bijlage XII-A)
- Protocol beveiligingsincidenten (bijlage XII-B)
- Formulier gegevens datalek (bijlage XII-C)
- Meldformulier (bijlage XII-D)
- Registratie datalekken (bijlage XII-E)

Artikel 3. De functionaris gegevensbescherming (FG)

3.1. De FG vervult zijn taken en verplichtingen onafhankelijk van het bestuur.

3.2. De FG houdt intern toezicht op de naleving van de wet- en regelgeving, de in de onderwijssector vastgestelde gedragscodes, het beleid van de Stichting of de verwerker met betrekking tot de bescherming van persoonsgegevens.

3.3. De FG adviseert over verwerkingsprocessen en ziet toe op de uitvoering en evaluatie ervan.

3.4. De FG adviseert over het passende niveau van beveiliging van de informatiehuishouding in de organisatie en over maatregelen die zijn gericht op het beperken van de verwerking van persoonsgegevens.

3.5. De FG werkt samen met de toezichthoudende autoriteit (Autoriteit Persoonsgegevens).

3.6. Betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten op grond van dit reglement en uit hoofde van de Verordening.

3.7. De FG brengt jaarlijks verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden en bevindingen.

3.8. De FG is met betrekking tot zijn taken tot geheimhouding en vertrouwelijkheid gehouden.

Artikel 4. Informatie en toegang tot de persoonsgegevens

4.1. Indien de gegevens van de betrokkene zelf worden verkregen, informeert de Stichting betrokkene bij de verkrijging van de persoonsgegevens over:

a. de volledige naam en de contactgegevens van de Stichting alsmede van de Functionaris Gegevensbescherming;
b. de doeleinden waarvoor de persoonsgegevens worden verwerkt;
c. de wettelijke grondslag voor de verwerking, en indien de verwerking is gebaseerd op de grondslag gerechtvaardigd belang (artikel 6 lid 1f AVG), het gerechtvaardigd belang van de Stichting;
d. de ontvangers of categorieën van ontvangers;
e. in voorkomend geval, dat de Stichting het voornemen heeft om de persoonsgegevens door te geven aan een derde land of internationale organisatie, om welk derde land het gaat en of het niveau van gegevensbescherming in dit land adequaat is, dan wel of er passende waarborgen zijn genomen;
f. hoelang de persoonsgegevens worden bewaard;
g. het recht van betrokkene om te verzoeken om inzage, rectificatie, beperking van de verwerking en wissing van de persoonsgegevens, alsmede het recht om bezwaar te maken tegen de verwerking;
h. het recht van betrokkene om te allen tijde eerder gegeven toestemming in te trekken;
i. het recht van betrokkene om een klacht in te dienen bij de AP;
j. het bestaan van automatische besluitvorming en de onderliggende logica hiervan, alsmede het belang en de verwachte gevolgen van de verwerking voor betrokkene; en
k. of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn als de betrokkene de gegevens niet verstrekt.

4.2. Indien de gegevens *niet* van betrokkene afkomstig zijn verstrekt de Stichting aan de betrokkene de informatie als genoemd onder 4.1. a. t/m j. en in aanvulling daarop informatie over: - de betrokken categorieën van persoonsgegevens; en

- de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

De Stichting verstrekt deze informatie binnen een redelijke termijn, doch uiterlijk binnen één maand na de verkrijging van de persoonsgegevens. Indien de gegevens worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene. Indien de verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

4.3. Een ieder die betrokken is bij de uitvoering van dit reglement en daarbij de toegang krijgt tot persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan en tekent de geheimhoudingsverklaring. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

Beleidskader

- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Brondocumenten/ brongegevens en bewaartermijnen (bijlage I-B))
- Geheimhoudingsverklaring (bijlage IV)
- Toestemmingsformulier oud-personeelsleden (bijlage V-A)
- Toestemmingsformulier oud-leerlingen (bijlage V-B)
- Privacy statement bezoekers website (bijlage VI)
- Privacyverklaring (bijlage VIII)

Artikel 5. Categorieën van betrokkenen, doeleinden en persoonsgegevens

5.1. Leerlingen

5.1.1. De verwerking van persoonsgegevens van leerlingen heeft ten doel:

a. de toelating en inschrijving van de leerling bij de school (artikel 6 lid 1b);

b. de organisatie of het geven van het onderwijs, de (individuele) schoolbegeleiding van leerlingen, het opstellen van een onderwijskundig rapport en het geven van studieadviezen (artikel 6 lid 1c AVG);

c. het bij uitschrijving van een leerplichtige leerling informeren van de vervolgschool over het gevolgde onderwijs en de behaalde studieresultaten (artikel 6 lid 1c AVG); d. het gebruik van een leerlingvolgsysteem dat de school inzicht verschaft in de cognitieve en sociaal-emotionele ontwikkeling en mogelijkheid biedt tot beheer en delen van deze gegevens met de docenten van de leerlingen en de ouders/verzorgers en leerlingen (artikel 6 lid 1c AVG);

e. het uitvoeren van de op de Stichting rustende verplichtingen en bevoegdheden op grond van de wet en daarop gebaseerde uitvoeringsregelgeving, waaronder (doch niet uitsluitend) de Wet op het voortgezet onderwijs (Wvo), de Wet op het primair onderwijs (Wpo), de Wet Medezeggenschap scholen (WMS), de Leerplichtwet en daarop gebaseerde regelgeving (artikel 6 lid 1c en 1e AVG);

f. het verstrekken of ter beschikking stellen van leermiddelen (artikel 6 lid 1c AVG);

g. het geven van onderwijs met behulp van digitale leermiddelen en diensten van de informatiemaatschappij (artikel 6 lid 1a AVG);

h. het verstrekken van inloggegevens voor het schoolnetwerk en digitale leermiddelen en – diensten (artikel 6 lid 1b AVG);

i. het berekenen en vaststellen van ouderbijdragen (artikel 6 lid 1b AVG);

j. het behandelen van geschillen aanhangig gemaakt bij klachten- en geschillencommissies (artikel 6 lid 1c AVG);
k. het laten uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
l. het medewerking verlenen aan een aanvraag van ouders, respectievelijk leerlingen, van leerlingenvervoer (artikel 6 lid 1c AVG);
m. het bekend maken van informatie over de organisatie, de activiteiten van de school in de schoolgids, op de website en sociale media (artikel 6 lid 1a AVG);
n. het opstellen en vormgeven van een (digitaal) smoelenboek met de foto's van leerlingen (artikel 6 lid 1a AVG);
o. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting, waaronder in ieder geval het verstrekken van een leerlingpas (artikel 6 lid 1f AVG);
p. het uitvoering geven aan de wettelijke verplichting gegevens te verstrekken aan het Ministerie van Onderwijs en Wetenschappen, de onderwijsinspectie, en overige instanties, waaronder maar niet uitsluitend de instanties die onderdeel uitmaken van het Zorgadviesteam (ZAT) voor zover de verplichting daartoe voortvloeit uit de wetgeving, inclusief de op de onderwijswetgeving gebaseerde bekostigingsvoorwaarden
(artikel 6 lid 1c AVG);
q. het voldoen aan een verzoek van een bestuursorgaan dat is belast met de uitvoering van een publiekrechtelijke taak (artikel 6 lid 1e AVG);
r. het aanbieden van diensten door de schoolfotograaf (artikel 6 lid 1a AVG).

5.1.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens zoals het e-mailadres, alsmede het bankrekeningnummer van de betrokkene;
b. het BSN-nummer;
c. nationaliteit en geboorteplaats;
d. persoonsgebonden leerlingnummer;
e. gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling;
f. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het onderwijs;
g. gegevens over de leerresultaten, waaronder maar niet uitsluitend gerekend worden test- en toetsgegevens, gegevens betreffende de aard en het verloop van het onderwijs, zaken die volgens de basisschool van invloed kunnen zijn op de prestaties in het voortgezet onderwijs, verzuim en afwezigheid van de leerling, de diagnostische eindtoets, het werk van het centraal examen en de rekentoets;
h. gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van (digitale) leermiddelen;
i. gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, ouderbijdragen, vergoedingen voor leermiddelen en buitenschoolse activiteiten;
j. foto's en videobeelden met of zonder geluid van (les)activiteiten van de school;
k. (digitale) pasfoto's;

l. inloggegevens voor het schoolnetwerk, de door de school gebruikte digitale leermiddelen, sociale media en software applicaties voor onderwijsdoeleinden alsmede inlogcodes voor de bestelling van reguliere leermiddelen bij de leverancier;

m. gegevens als bedoeld onder a. en c., van de ouders, voogden of verzorgers van leerlingen en of sprake is van gezamenlijk ouderlijk gezag en gegevens over lidmaatschap van de ouderraad of de oudergeleding van de medezeggenschapsraad. [PO: beroep of hoogst genoten opleidingsniveau];

n. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;

o. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;

p. andere dan de onder a. tot en met o. bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een wettelijke regeling.

5.2. Personeel

5.2.1. De verwerking van gegevens van personeel heeft ten doel:

a. het aangaan van de arbeidsovereenkomst (artikel 6 lid 1b AVG);

b. het vaststellen van het salaris en overige arbeidsvoorwaarden (artikel 6 lid 1b AVG);

c. het (laten) uitbetalen van salaris, de afdracht van belastingen en premies (artikelen 6 lid 1b en 6 lid 1c AVG);

d. de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde (artikel 6 lid 1b AVG);

e. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen (artikel 6 lid 1b AVG);

f. het verlenen van ontslag (artikel 6 lid 1b AVG);

g. de overgang van de betrokkene naar diens (tijdelijke) tewerkstelling bij een ander onderdeel van de groep, bedoeld in artikel 2:24b van het Burgerlijk Wetboek waaraan de verwerkingsverantwoordelijke is verbonden (artikel 6 lid 1b AVG);

h. het geven van leiding en het begeleiden van betrokkene (artikel 6 lid 1b AVG);

i. het verstrekken van de bedrijfsmedische zorg voor betrokkene en het kunnen nakomen van re-integratieverplichtingen bij verzuim (artikel 6 lid 1c AVG);

j. het toegang verlenen tot het schoolnetwerk (artikel 6 lid 1b AVG);

k. het regelen van en de controle van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband (artikel 6 lid 1b AVG);

l. de verkiezing van de leden van een bij wet geregeld medezeggenschapsorgaan (artikel 6 lid 1c AVG);

m. het behandelen van geschillen (artikel 6 lid 1b AVG);

n. de behandeling van personeelszaken, anders dan genoemd onder a. t/m m. (artikel 6 lid 1b AVG);

o. de organisatie of het geven van het onderwijs (artikel 6 lid 1b AVG);

p. het laten uitoefenen van accountantscontrole en het laten vaststellen van aanspraken op bekostiging (artikel 6 lid 1c AVG);

q. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG);

5.2.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;
b. BSN-nummer;
c. kopie ID-bewijs/paspoort;
d. een personeelsnummer dat geen andere informatie bevat dan bedoeld onder a;
e. nationaliteit, geboorteplaats;
f. gegevens betreffende de godsdienst of levensovertuiging, voor zover die noodzakelijk zijn voor een goede functie-uitoefening conform de benoemingsvoorwaarden;
g. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
h. gegevens betreffende de arbeidsvoorwaarden;
i. gegevens betreffende het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura;
j. gegevens betreffende het berekenen, vastleggen en betalen van belasting en premies;
k. gegevens betreffende de functie of de voormalige functie(s), alsmede betreffende de aard, de inhoud en de beëindiging van voorgaande dienstverbanden;
l. gegevens met het oog op de administratie van de aanwezigheid van de betrokkenen op de plaats waar de arbeid wordt verricht en hun afwezigheid in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte;
m. gegevens die in het belang van de betrokkenen worden opgenomen met het oog op hun arbeidsomstandigheden en veiligheid;
n. gegevens, waaronder begrepen gegevens betreffende gezinsleden en voormalige gezinsleden van de betrokkenen, die noodzakelijk zijn met het oog op een overeengekomen arbeidsvoorwaarden;
o. gegevens met betrekking tot de functie-uitoefening, de personeelsbeoordeling en de loopbaanbegeleiding, voor zover die gegevens bij de betrokkenen bekend zijn;
p. gegevens van docenten, onderwijsondersteunend personeel en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van de school of de instelling en het geven van onderwijs, opleidingen en trainingen;
q. inloggegevens van het schoolnetwerk en digitale leermiddelen;
r. foto's en videobeelden met of zonder geluid van activiteiten van de school en van lessen van onderwijzend personeel;
s. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;;
t. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
u. andere dan de onder a. tot en met t. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere niet nader genoemde wet.

5.3. Sollicitanten

5.3.1. De Stichting heeft een sollicitatiecode waarin de procedures van de organisatie inzake werving en selectie zijn opgenomen als ook de wijze van omgang met persoonsgegevens.

5.3.2. De verwerking van gegevens van sollicitanten heeft ten doel:

a. de beoordeling van de geschiktheid van betrokkene voor een functie die vacant is (artikelen 6 lid 1a en 6 lid 1b AVG);
b. de beoordeling van de geschiktheid van betrokkene voor een functie die in de nabije toekomst vacant kan komen (artikelen 6 lid 1a en 6 lid 1b AVG);
c. de afhandeling van de door de sollicitant gemaakte onkosten (artikel 6 lid 1a AVG);
d. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG);
e. de uitvoering of toepassing van wetgeving (artikel 6 lid 1c AVG).

5.3.3. Geen andere gegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;
b. nationaliteit en geboorteplaats;
c. gegevens betreffende de godsdienst of levensovertuiging, voor zover die noodzakelijk zijn voor de beoordeling of de sollicitant voldoet aan de benoemingsvoorwaarden;
d. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
e. gegevens betreffende de functie waarnaar gesolliciteerd is;
f. gegevens betreffende de aard en inhoud van de huidige dienstbetrekking, alsmede betreffende de beëindiging ervan;
g. gegevens betreffende de aard en inhoud van de vorige dienstbetrekkingen, alsmede betreffende de beëindiging ervan;
h. andere gegevens met het oog op het vervullen van de functie (bijvoorbeeld gegevens in het kader van een te voeren voorkeursbeleid voor minderheden of re-integratiebeleid);
i. foto's en videobeelden met of zonder geluid;
j. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;
k. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
l. andere gegevens met het oog op het vervullen van de functie, die door of na toestemming van de betrokkene zijn verstrekt (assessments, psychologisch onderzoek, uitslag medische keuring);
m. andere dan de onder a. tot en met j. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet;
n. gegevens verkregen uit internetsearch.

5.4. Oud-medewerkers

5.4.1. De verwerking van gegevens van oud-medewerkers heeft ten doel:

a. het onderhouden van contacten met oud-medewerkers (artikel 6 lid 1a AVG);
b. het verzenden van informatie aan oud-medewerkers (artikel 6 lid 1a AVG);
c. het verwerken van de aanmeldingen van oud-medewerkers voor mede voor hen georganiseerde activiteiten en bijeenkomsten (artikel 6 lid 1a AVG);
d. het berekenen, vastleggen en innen van bijdragen en giften, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede andere activiteiten van intern beheer (artikel 6 lid 1a AVG);

e. het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG).

5.4.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;
b. gegevens betreffende de functie waarin en de periode gedurende welke de oud-medewerker voor de verwerkingsverantwoordelijke werkzaam is geweest;
c. gegevens met het oog op het berekenen, vastleggen en innen van bijdragen en giften;
d. een administratiecode dat geen andere informatie bevat dan bedoeld onder a. tot en met c.;
e. gegevens met betrekking tot aanmelding activiteiten/bijeenkomsten.

5.5. Oud-leerlingen

5.5.1. De verwerking van gegevens van oud-leerlingen heeft ten doel:

a. het onderhouden van contacten met de oud-leerlingen (artikel 6 lid 1a AVG);
b. het verzenden van informatie aan de oud-leerlingen (artikel 6 lid 1a AVG);
c. het verwerken van de aanmeldingen van oud-leerlingen voor mede voor hen georganiseerde activiteiten en bijeenkomsten (artikel 6 lid 1a AVG);
d. het berekenen, vastleggen en innen van bijdragen en giften, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede andere activiteiten van intern beheer (artikel 6 lid 1a AVG);
e. het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
f. het archiefbeheer, het behandelen van geschillen, het verrichten van wetenschappelijk, statistisch of historisch onderzoek (artikel 6 lid 1a en artikel 6 lid 1f AVG).

5.5.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens, zoals het e-mailadres alsmede bankrekeningnummer van de betrokkene;
b. gegevens betreffende de aard van de (vervolg) studie respectievelijk toekomstige werkkring en de periode gedurende welke de oud-leerling, de opleiding heeft gevolgd;
c. gegevens met het oog op het berekenen, vastleggen en innen van bijdragen en giften;
d. een administratiecode dat geen andere informatie bevat dan bedoeld onder a. tot en met c.;
e. gegevens met betrekking tot aanmelding activiteiten/bijeenkomsten.

5.6. Leden van het toezichthoudend orgaan

5.6.1. De verwerking van gegevens van de (kandidaat-)leden van het toezichthoudend orgaan heeft ten doel:

a. het vastleggen van de benoeming, de functie binnen het toezichthoudend orgaan en de benoemingstermijn (artikel 6 lid 1b AVG);
b. het vastleggen en (laten) uitbetalen van de – door het toezichthoudend orgaan - vastgestelde beloning alsmede overige activiteiten van intern beheer (artikel 6 lid 1b AVG);
c. de aanmelding voor de aansprakelijkheidsverzekering voor toezichthouders (artikel

6 lid 1b AVG);

d. het uitvoering geven aan het recht van de medezeggenschapsraad om op grond van de WMS een bindende voordracht te doen voor een toezichthouder (artikel 6 lid 1c AVG);
e. de organisatie van de school waaronder het informeren van personeel en leerlingen over de samenstelling en bereikbaarheid van het toezichthoudend orgaan (artikel 6 lid 1b AVG);
f. het onderhouden van contacten tussen de Stichting en de medezeggenschapsraad met het toezichthoudend orgaan (artikel 6 lid 1b AVG);
g. het verzenden van (management)informatie aan het toezichthoudend orgaan (artikel 6 lid 1 b AVG);
h. het laten uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
i. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting] (artikel 6 lid 1f AVG).

5.6.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;
b. BSN-nummer;
c. kopie ID-bewijs/paspoort;
d. nationaliteit en geboorteplaats;
e. gegevens betreffende de godsdienst of levensovertuiging, voor zover die noodzakelijk zijn voor een goede functie-uitoefening conform de benoemingsvoorwaarden;
f. gegevens betreffende het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura;
g. gegevens betreffende gevolgde en te volgen opleidingen;
h. gegevens betreffende de functie binnen het toezichthoudend orgaan, alsmede betreffende de aard, de inhoud van de overige werkzaamheden en expertise;
i. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;;
j. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
k. andere dan de onder a. tot en met i. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere niet nader genoemde wet.

5.7. Bezoekers

5.7.1. De verwerking van gegevens van bezoekers van een van de schoolgebouwen van de Stichting heeft ten doel:

a. het interne beheer (artikel 6 lid 1f AVG);
b. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG).

5.7.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde

gegevens, zoals het e-mailadres alsmede de organisatie waartoe de bezoeker behoort;

b. een administratienummer dat geen andere informatie bevat dan onder a.;
c. gegevens betreffende de persoon en afdeling die de betrokkene wenst te bezoeken;
d. gegevens betreffende de reden van het bezoek;
e. gegevens betreffende de datum en het tijdstip van de aankomst en het vertrek van de bezoeker;
f. gegevens inzake het identiteitsbewijs van de bezoeker;
g. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;
h. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt.

5.7.3. Website

De Stichting informeert bezoekers van de website van de Stichting bij een bezoek aan de website over de doeleinden en gegevens die worden verwerkt bij een bezoek aan de website door middel van een privacy statement dat op de website van de Stichting is geplaatst.

5.8. Leveranciers/dienstverleners

5.8.1. De verwerking van gegevens van leveranciers van de Stichting heeft ten doel:

a. het doen van bestellingen of de opdrachtverlening aan dienstverleners (artikel 6 lid 1b AVG);
b. het berekenen en vastleggen van inkomsten en uitgaven en het doen van betalingen (artikel 6 lid 1b AVG);
c. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen alsmede andere activiteiten van intern beheer (artikel 6 lid 1b AVG);
d. het onderhouden van contacten door de verwerkingsverantwoordelijke met de leveranciers (artikel 6 lid 1b AVG);
e. het behandelen van geschillen en het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
f. de uitvoering of de toepassing van een andere wet (artikel 6 lid 1c AVG);
g. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG).

5.8.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede de organisatie waartoe de betrokkene behoort;
b. een administratienummer dat geen andere informatie bevat dan onder a.;
c. gegevens met het oog op het doen van bestellingen of het opdracht verlenen aan dienstverleners;
d. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;

e. andere dan de onder a. tot en met d. bedoelde gegevens waarvan de verwerking is vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet;

f. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt.

5.9. Huurders

5.9.1. De verwerking van gegevens van huurders van de Stichting heeft ten doel:

a. de uitvoering van de overeenkomst (artikel 6 lid 1 b AVG);

b. het berekenen en vastleggen van inkomsten en uitgaven en het doen van betalingen (artikel 6 lid 1b AVG);

c. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen (artikel 6 lid 1b AVG);

d. het behandelen van geschillen en het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);

e. activiteiten van intern beheer, beveiliging van en toezicht op personen, zaken en goederen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG);

f. de uitvoering of toepassing van wet- en regelgeving (artikel 6 lid 1c AVG).

5.9.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede de organisatie waartoe de betrokkene behoort;

b. een administratienummer dat geen andere informatie bevat dan onder a.;

c. gegevens die noodzakelijk zijn voor de uitvoering van de huurovereenkomst;

d. gegevens met het oog op het berekenen en vastleggen van inkomsten en uitgaven, het doen van betalingen en het innen van vorderingen;

e. gegevens betreffende de datum en het tijdstip van de aankomst en het vertrek van de betrokkene;

f. gegevens inzake het identiteitsbewijs van de betrokkene;

g. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;

h. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt.

Beleidskader

- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Brondocumenten/ brongegevens en bewaartermijnen (bijlage I-B)
- Toestemmingsformulier oud-personeelsleden (bijlage V-A)
- Toestemmingsformulier oud-leerlingen (bijlage V-B)
- Privacy statement bezoekers website (bijlage X)
- Privacyverklaring (bijlage VI)

Artikel 6. Rechten betrokkenen

6.1. Privacyverklaring

6.1.1. De Stichting beschikt over een privacyverklaring, waarin betrokkenen in duidelijke, begrijpelijke en gemakkelijk toegankelijke vorm, in het bijzonder wanneer de informatie specifiek voor de leerling is, worden geïnformeerd over de gegevens die van hem worden verwerkt, de wijze waarop, en de redenen waarom dit gebeurt.

6.2. Recht op informatie

6.2.1. Betrokkenen van wie persoonsgegevens worden verwerkt, dan wel - indien zij de leeftijd van zestien jaar nog niet bereikt hebben - hun wettelijke vertegenwoordigers, hebben het recht van inzage in, en recht op een kopie van, de over hen, respectievelijk hun pupil, opgenomen gegevens en van de volgende informatie over:

a. de verwerkingsdoeleinden en de rechtsgrond voor de verwerking;
b. de betrokken categorieën van persoonsgegevens;
c. de ontvangers en/of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
d. de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen of indien dat niet mogelijk is de criteria om die termijn te bepalen;
e. de herkomst van de verwerkte gegevens indien deze niet van betrokkene afkomstig zijn;
f. het bestaan van geautomatiseerde besluitvorming, alsmede het belang en de verwachte gevolgen van die verwerking voor betrokkene.

6.3. Recht op rectificatie en wissing

6.3.1. Betrokkenen hebben het recht op rectificatie van onjuiste persoonsgegevens.

6.3.2. Betrokkenen hebben recht op wissing van gegevens ('recht op vergetelheid') in de volgende situaties:

a. de persoonsgegevens zijn niet langer nodig;
b. de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 5 lid 2.a. berust in en er is geen andere rechtsgrond voor die verwerking;
c. de betrokkene maakt bezwaar tegen de verwerking en er zijn geen prevalerende dwingende vormen voor verwerking;
d. de gegevens zijn onrechtmatig verwerkt;
e. er is een wettelijke verplichting om de persoonsgegevens te wissen;
f. de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

6.3.3. In het geval de te wissen gegevens openbaar zijn gemaakt en de Stichting besluit de gegevens te wissen, neemt de Stichting, rekening houdend met de beschikbare technologie en uitvoeringskosten redelijke maatregelen waaronder technische maatregelen, om andere verwerkingsverantwoordelijken ervan op de hoogte te stellen dat de betrokkene heeft verzocht om iedere koppeling naar of kopie of reproductie van die gegevens te wissen.

6.3.4. Artikel 6.3.1 en 6.3.2 zijn niet van toepassing als de verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting of voor het nakomen van een wettelijke verwerkingsverplichting, of voor het vervullen van een taak van algemeen belang, om

redenen van algemeen belang op het gebied van volksgezondheid, met het oog op archivering in het algemeen belang wetenschappelijk of historisch onderzoek, voor zover het in 6.3.1 en 6.3.2. bedoelde recht de verwezenlijking van de deze doeleinden onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

6.4. Recht op beperking van verwerking van gegevens

6.4.1. Betrokkene heeft op grond van de verordening in nader bepaalde situaties een recht op beperking van de verwerking van zijn gegevens. Dit houdt in dat de Stichting de persoonsgegevens, met uitzondering van de opslag, slechts verwerkt met toestemming van betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een ander natuurlijk persoon of rechtspersoon of om gewichtige redenen van algemeen belang.

6.5. Recht op overdraagbaarheid van gegevens

6.5.1. Betrokkene heeft recht de hem betreffende persoonsgegevens die hij zelf aan de Stichting heeft verstrekt in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen in de gevallen dat persoonsgegevens door hem op basis van verleende toestemming (artikel 6 lid 1a AVG) zijn verstrekt of op basis van een overeenkomst (artikel 6 lid 1b AVG) en de verwerking via geautomatiseerde procedés wordt verricht.

6.5.2. Bij de uitoefening van zijn recht op gegevensoverdraagbaarheid uit hoofde van het vorige lid heeft de betrokkene het recht dat gegevens indien dit technisch mogelijk is rechtstreeks van de ene naar de andere verwerkingsverantwoordelijke worden doorgezonden.

6.5.3. Het recht geldt niet voor verwerkingen die noodzakelijk zijn 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 de verwerkingsverantwoordelijke is verleend.

6.6. Indiening van een verzoek

6.6.1. Een verzoek als bedoeld in dit artikel wordt gericht aan de functionaris gegevensbescherming.Contactgegevens zijn te vinden op de website van de scholengroep.

6.6.2. Aan een verzoek zijn geen kosten verbonden. Wanneer verzoeken van een betrokkene kennelijk ongegrond, of buitensporig zijn, met name vanwege hun repetitieve karakter kan de Stichting echter:

- een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verzoek gepaard gaat; ofwel
- weigeren gevolg geven aan het verzoek.

6.6.3. De Stichting verstrekt de betrokkene binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven.

6.6.4. Indien de betrokkene een verzoek doet omdat bepaalde opgenomen gegevens onjuist c.q. onvolledig zouden zijn, hij een belang heeft bij beëindiging van de verwerking dat zwaarder weegt dan dat van de organisatie, dan wel de verwerking gezien de doelstelling van het reglement niet (langer) noodzakelijk is, dan wel strijdig zijn met dit reglement, neemt de functionaris gegevensbescherming namens de verwerkingsverantwoordelijke binnen een maand nadat betrokkene dit verzoek heeft ingediend, hierover een schriftelijke beslissing.

6.6.5. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De Stichting stelt de betrokkene

binnen een maand in kennis van een dergelijke verlenging. Wanneer betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

6.6.6. Indien de Stichting twijfelt aan de identiteit van de verzoeker, vraagt hij zo spoedig mogelijk aan de verzoeker schriftelijk nadere gegevens inzake zijn identiteit te verstrekken of een geldig identiteitsbewijs te overleggen. Door dit verzoek wordt de termijn opgeschort tot het tijdstip dat het gevraagde bewijs is geleverd.

6.6.7. Indien de Stichting geen gevolg wenst te geven aan een verzoek als bedoeld in dit artikel doet hij hiervan – gemotiveerd - schriftelijk mededeling aan de betrokkene, binnen een maand na ontvangst van het verzoek.

6.7. Beperkingen

6.7.1. De reikwijdte van verplichtingen van de Stichting enerzijds en de rechten van betrokkene anderzijds kunnen zijn beperkt op grond van wet- en regelgeving die op de Stichting en/of zijn verwerkers van toepassing zijn.

6.8. Recht op het indienen van een klacht

6.8.1. De betrokkene die zich niet kan verenigen met de afwijzing van zijn verzoek als bedoeld in dit artikel kan zich wenden tot de externe klachtencommissie zoals bedoeld in de klachtenregeling van de Stichting of de Autoriteit Persoonsgegevens benaderen met een verzoek tot bemiddeling.

Beleidskader

- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Brondocumenten/ brongegevens en bewaartermijnen (bijlage I-B)
- Privacyverklaring (bijlage VIII)

Artikel 7. Beveiliging

7.1. De Stichting hanteert het voor de onderwijssector vastgestelde normenkader bij het vaststellen van passende technische en organisatorische maatregelen waartoe de Verordening verplicht.

7.2. De Stichting treft maatregelen die een effectief beschermingsniveau bieden, afhankelijk van de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Daarbij rekening houdend met de stand van de techniek en de uitvoeringskosten. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Beleidskader

- Toestemmingsformulier oud-personeelsleden (bijlage V-A)
- Toestemmingsformulier oud-leerlingen (bijlage V-B)
- Protocol gebruik van e-mail, internet en sociale media (bijlage II)
- Protocol gebruik van camera- en videobeelden (bijlage III)
- Geheimhoudingsverklaring (bijlage IV)
- Normenkader saMBO-ICT, bron: saMBO-ICT (bijlage VIII
- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Brondocumenten/ brongegevens en bewaartermijnen (bijlage I-B)
- Handboek datalekken (bijlage VII- A t/m E)

Artikel 8. De verwerker

8.1. De verwerkers zijn degenen die op basis van een overeenkomst voor of namens de Stichting gegevens verwerken.

8.2. De verwerker verwerkt de gegevens op de wijze zoals overeengekomen in een verwerkersovereenkomst tenzij de verwerker die gegevens verwerkt bij het gebruik van leermiddelen, toetsen, school- en leerlinginformatiemiddelen (zoals gedefinieerd in de Model Verwerkersovereenkomst behorend bij het Convenant Digitale Onderwijsmiddelen). In dat geval verwerkt de verwerker de gegevens zoals voorgeschreven in de Model Verwerkersovereenkomst eventueel met inachtneming van de aanvullingen en wijzigingen zoals opgenomen in bijlage 3 behorend bij de model verwerkersovereenkomst.

8.3. De verwerker is verantwoordelijk voor het juiste gebruik van de nodige voorzieningen om de bescherming van de persoonlijke levenssfeer van de personen van wie gegevens in de persoonsregistratie zijn opgenomen, in voldoende mate te waarborgen, zoals aangegeven en beschreven in de verwerkersovereenkomst.

8.4. De functionaris gegevensbescherming ziet erop toe dat de in het vorige lid bedoelde voorzieningen worden getroffen en in acht worden genomen.

Beleidskader

- Geheimhoudingsverklaring (bijlage IV)
- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Handboek datalekken (bijlage (bijlage VII- A t/m E))

Artikel 9. Inbreuk op de beveiliging

9.1. Indien zich binnen de organisatie van de Stichting of bij een door de Stichting ingeschakelde verwerker een inbreuk op de beveiliging voordoet, waarbij een aanzienlijke kans bestaat op

verlies of onrechtmatige verwerking van persoonsgegevens die door de Stichting worden verwerkt, dan wel dit verlies of onrechtmatige verwerking zich daadwerkelijk voordoet, zal de Stichting daarvan melding doen bij de Autoriteit Persoonsgegevens, tenzij kan worden aangetoond dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich brengt.

9.2. De Stichting zal iedere inbreuk op de beveiliging als bedoeld in artikel 9.1. documenteren, ongeacht of deze wordt gemeld bij de AP.

9.3. Indien de inbreuk een hoog risico voor de rechten en vrijheden van betrokkene inhoudt, stelt de Stichting ook de betrokkene onverwijld in kennis van de inbreuk. Deze mededeling kan achterwege blijven indien:

- de persoonsgegevens versleuteld zijn en niet toegankelijk voor derden;
- er inmiddels maatregelen getroffen zijn die het hoge risico hebben weggenomen;
- de mededeling een onevenredige inspanning vergt. Een openbare mededeling kan dan volstaan.

9.4. Bij het vaststellen of sprake is van een inbreuk op de beveiliging en of melding daarvan moet worden gedaan bij de Autoriteit Persoonsgegevens hanteert de Stichting de procedures die zijn opgenomen in het handboek en protocol Datalekken.

Beleidskader

- Overzicht van toegangsrechten interne verwerkers (bijlage I-A)
- Handboek datalekken (bijlage VII- A t/m E)

Artikel 10. Klachten

10.1. Indien de betrokkene van mening is dat de bepalingen van de Verordening en overige wet- en regelgeving en (onderwijs)gedragscodes zoals uitgewerkt in dit reglement niet door de instelling worden nageleefd dient hij/zij zich te wenden tot de FG.

10.2. Indien de ingediende klacht voor de betrokkene niet leidt tot een voor hem/haar acceptabel resultaat, kan hij zich wenden tot de Autoriteit Persoonsgegevens dan wel tot de rechter.

10.3. (Ouders/verzorgers van) leerlingen en medewerkers kunnen zich tevens wenden tot de externe klachtencommissie waarbij de Stichting is aangesloten. Voor contactgegevens klachtencommissie GCBO, zie website en intranet.

Beleidskader

- Klachtenregeling en rol vertrouwenspersonen voor de scholen van sg. OMB VO - PO
- Reglement landelijke klachtencommissie GCBO VO – PO
- Regeling inzake het omgaan met een vermoeden van een ernstige misstand (klokkenluidersregeling)
- Klachtformulier AP: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-over-gebruik-persoonsgegevens
- Privacyverklaring (bijlage VIII)

Artikel 11. Inwerkingtreding, wijziging en citeertitel

11.1. Dit reglement kan aangehaald worden als '*Privacyreglement'* en treedt in werking op de datum vermeld op het titelblad.

11.2. Het reglement is vastgesteld door de Stichting en de gemeenschappelijke medezeggenschapsraad en vervangt eventuele vorige versies.

11.3. Het reglement zal periodiek worden geëvalueerd met alle geledingen van De gemeenschappelijke medezeggenschapsraad en kan indien dit wordt gewenst of nodig is om de AVG correct na te leven, worden gewijzigd, nadat instemming van de gemeenschappelijke medezeggenschapsraad is verkregen.

Bijlagenoverzicht

Bijlage I	A. Overzicht van toegangsrechten interne verwerkers B. Brondocumenten/brongegevens en bewaartermijnen
Bijlage II	Protocol gebruik van e-mail, ICT en sociale media
Bijlage III	Protocol gebruik van camera- en videobeelden
Bijlage IV	Geheimhoudingsverklaring
Bijlage V	A. Toestemmingsformulier oud-personeelsleden B. Toestemmingsformulier oud-leerlingen
Bijlage VI	Privacy statement bezoekers website
Bijlage VII	A. Handboek datalekken B. Protocol beveiligingsincidenten C. Formulier gegevens datalek D. Meldformulier E. Registratie datalekken
Bijlage VIII	Privacyverklaring

Artikelsgewijze toelichting ten behoeve van implementatie van het reglement

Artikel 1. Begripsbepalingen

De meeste begripsbepalingen vloeien direct voort uit de AVG, de Wet op het primair onderwijs, de Wet op het voortgezet onderwijs en de Wet op de expertisecentra.

Autoriteit Persoonsgegevens (AP)

De Autoriteit Persoonsgegevens ziet, op grond van de AVG, als onafhankelijke instantie erop toe, dat persoonsgegevens zorgvuldig worden gebruikt en beveiligd en dat de privacy van burgers gewaarborgd blijft. Wanneer een organisatie zich niet houdt aan de wet, kan de autoriteit maatregelen nemen. De AP kan ook boetes opleggen.

Betrokkene

De persoon wiens gegevens worden verwerkt, wordt in de AVG 'de betrokkene' genoemd. Indien de school ook gegevens van andere betrokkenen (bijvoorbeeld: donateurs etc.) verwerkt, dient het modelreglement daarop te worden aangepast.

Dienst van de informatiemaatschappij

Kortgezegd iedere internetdienst (bijvoorbeeld: digitale leermiddelen, spellingapps, etc.). Een dienst is een dienst van de informatiemaatschappij als de dienst elektronisch wordt geleverd zonder dat de aanbiedende partij en ontvangende partij gelijktijdig aanwezig zijn en de dienst enkel wordt geleverd omdat de afnemer (school/docent/leerling) daarom vraagt.

Leerling- of personeelsnummer

Niet zijnde het Burgerservicenummer. Een nummer dat binnen de administratie verwijst naar de gegevens van één persoon en dat wordt gebruikt om die gegevens op effectieve en efficiënte wijze te kunnen raadplegen en verwerken. Hiermee kunnen de persoonsgegevens die worden verwerkt van een persoon worden geminimaliseerd. Het leerling- en personeelsnummer kan dan dienen als koppelinstrument tussen de verschillende bestanden/verwerkingen zonder dat steeds de naam, etc. van de betrokkenen hoeft te worden verwerkt.

In dit reglement wordt als mogelijkheid genoemd gegevens te verwerken op basis van een personeels- en leerlingnummer. Het gebruik van een persoonsgebonden nummer kan ertoe bijdragen dat minder gegevens van betrokkenen hoeven te worden verwerkt en dat de toegang tot vertrouwelijke gegevens binnen en buiten de organisatie eveneens tot een minimum kan worden beperkt. Deze gedachte ligt ook ten grondslag aan het wetsvoorstel '*Pseudonimisering leerlinggegevens'*. Met dit wetsvoorstel wordt het voor onderwijsinstellingen in alle sectoren mogelijk om het persoonsgebonden nummer van een onderwijsdeelnemer te gebruiken ten behoeve van het genereren van een pseudoniem voor deze onderwijsdeelnemer in het kader van de toegang tot en het gebruik van digitale leermiddelen alsmede het digitaal afnemen van toetsen. Daarnaast voorziet het wetsvoorstel in een grondslag om voor andere doeleinden andere pseudoniemen te genereren.

Personeel

Personen in dienst van of werkzaam (geweest) voor de Stichting: zij die ten behoeve van de [Stichting/Vereniging] werkzaamheden verrichten of hebben verricht. Hieronder vallen niet alleen de personen die een akte van benoeming/aanstelling hebben, maar ook uitzendkrachten, stagiaires, vrijwilligers, personen die bij de Stichting zijn gedetacheerd, ouders, oud-medewerkers, etc. Dienstverleners daarentegen zijn veelal verwerker (bijvoorbeeld het administratiekantoor) of medeverwerkingsverantwoordelijke (zoals de accountant). De arbodienst kan zowel worden aangemerkt als verwerker én verwerkingsverantwoordelijke.

Persoonsgegevens

Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon zijn persoonsgegevens in de zin van de AVG. Om te bepalen of een persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren.

De aard van sommige persoonsgegevens brengt met zich mee dat de verwerking ervan een grote inbreuk kan vormen op de persoonlijke levenssfeer van de betrokkene, omdat die gegevens gevoelige informatie over iemand verschaffen. De AVG noemt deze gegevens bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn alle persoonsgegevens die informatie verschaffen over iemands:

- godsdienst of levensovertuiging;
- ras (etniciteit of afkomst);
- genetische kenmerken;
- biometrische kenmerken;
- gezondheid;
- seksuele leven; en
- lidmaatschap van een vakvereniging.

Verder zijn bijzondere persoonsgegevens:

- strafrechtelijke persoonsgegevens; en
- persoonsgegevens over onrechtmatig of hinderlijk handelen waarvoor een verbod is opgelegd (bijvoorbeeld een straatverbod).

Hoofdregel is dat bijzondere persoonsgegevens niet mogen worden verwerkt. De AVG kent een aantal algemene en een aantal specifieke uitzonderingen op dit verbod. Voor het onderwijs is de belangrijkste dat verwerking van bijzondere persoonsgegevens op grond van de AVG is toegestaan indien de verwerking noodzakelijk is met het oog op het verstrekken van zorg, behandeling of het beheren van diensten dan wel op een andere wettelijke grondslag (uitvoeringswet AVG).

De verwerkingsverantwoordelijke dient aan te geven om welke gegevens het gaat. De AVG verplicht verwerkingsverantwoordelijken daarnaast om de gegevens te classificeren als openbaar, vertrouwelijk of gevoelig.

Stichting/Vereniging/ Bevoegd gezag

In dit reglement komt de term bevoegd gezag niet meer terug. Hoofdregel in de Wpo/Wvo is dat de rechtspersoon die de school in stand houdt het bevoegd gezag is tenzij de gemeente (of de gemeenschappelijke) regeling de school in eigen beheer in stand houdt (artikel 1 Wpo/Wvo).

Verwerker

Onderscheid wordt gemaakt tussen in- en externe verwerkers (in het register van verwerkingactiviteiten aangeduid als 'Ontvangers'). Interne verwerkers zijn het personeel van de Stichting. Externe verwerkers zijn bijvoorbeeld het administratiekantoor. Soms zijn externe verwerkers ook zelf verwerkingsverantwoordelijke met betrekking tot de persoonsgegevens, zoals de Arbodienst. Naast de taken die zij in opdracht en namens de verwerkingsverantwoordelijke uitvoeren op basis van de afgesloten overeenkomst, verwerken zij medische gegevens op basis van artikel 7:464 Burgerlijk Wetboek (BW), die de Wet Geneeskundige Behandelovereenkomst (WGBO) naar analogie van toepassing verklaart. Ratio van deze bepaling is dat de rechten van de patiënt niet alleen in zuiver contractuele behandelingssituaties, maar ook in andersoortige situaties waarin een patiënt wordt onderworpen aan een geneeskundige handeling bescherming behoeven.

Als besloten wordt om feitelijke handelingen met betrekking tot gegevensverwerking door een verwerker te laten verrichten, zal met die verwerker een relatie worden aangegaan. De AVG stelt

eisen aan de keuze van een verwerker en aan de manier waarop de relatie met die verwerker vastligt. De AVG eist in artikel 32 dat de onderdelen die betrekking hebben op de bescherming van persoonsgegevens en op de beveiligingsmaatregelen, schriftelijk worden vastgelegd.

Verwerking van persoonsgegevens

Het gaat erom of iemand enige feitelijke macht of invloed, al dan niet via een computersysteem, over de gegevens kan uitoefenen. Iemand moet een handeling met de gegevens kunnen verrichten. Als iemand geen macht of invloed kan uitoefenen op de persoonsgegevens, valt deze verwerking niet onder de AVG.

Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is de Stichting, dat wordt vertegenwoordigd door het college van bestuur van de Stichting.

Artikel 2. Verantwoordelijkheden

De AVG richt zich tot de verwerkingsverantwoordelijke, in casu het schoolbestuur dat verantwoordelijk is voor een gegevensbeschermingsbeleid conform de in dit artikel genoemde uitgangspunten. In het beleidskader wordt verwezen naar de beleidsdocumenten die daarbij ondersteunend kunnen zijn. In het beleidskader en in beleidsdocumenten zelf wordt ook verwezen naar producten en beleidsdocumenten ontwikkeld door Kennisnet met bronvermelding en de hyperlink waarmee de documenten op de website van Kennisnet zijn terug te vinden

Artikel 3. Functionaris gegevensbescherming (FG)

De verplichting tot het aanstellen van een FG geldt voor overheidsinstanties en publieke organisaties, ongeacht het type persoonsgegevens dat ze verwerken. Het kan dan bijvoorbeeld gaan om de Rijksoverheid, gemeenten of provincies maar ook om zorg- en onderwijsinstellingen. In de AVG wordt geen definitie gegeven van "overheidsinstantie of –orgaan". De Artikel 29-werkgroep (de gezamenlijke Europese toezichthouders) heeft een richtlijn gepubliceerd over het aanstellen van een FG. In deze richtlijn wordt voor het begrip "overheidsinstantie of –orgaan" verwezen naar de definitie van "publiekrechtelijke instelling". Een publiekrechtelijke instelling is een aanbestedende dienst in de zin van de Aanbestedingsrichtlijn. Op grond van die definitie en bijlage uit deze richtlijn, kan ook een bijzondere onderwijsinstelling worden gekwalificeerd als een aanbestedende dienst als de financiering van een school voor meer dan de helft van de begroting afkomstig is van de overheid. Een organisatie is overigens ook verplicht een FG aan te stellen als zij regelmatig en stelselmatig betrokkenen observeren. Scholen voldoen snel aan deze eis, aangezien zij vaak leerlingvolgsystemen gebruiken. Daarnaast heeft het verwerken van bijzondere en strafrechtelijke gegevens op 'grote schaal' ook tot gevolg dat een organisatie een FG moet aanstellen. Bijzondere persoonsgegevens zijn gegevens die iets zeggen over iemands ras, godsdienst, seksuele leven, politieke opvatting, gezondheid, maar ook genetische gegevens (zoals DNA) en biometrische gegevens (bijvoorbeeld vingerafdrukken). Elke onderwijsinstelling verwerkt in ieder geval enkele bijzondere persoonsgegevens van leerlingen in een onderwijskundig rapport. Bijvoorbeeld of een leerling ADHD heeft, dyslectisch of depressief is. Onderwijsinstellingen voldoen (in bijna alle gevallen) aan de drie verschillende vereisten om een FG aan te moeten stellen. Let op: het voldoen aan één van de drie vereisten is al genoeg om verplicht een FG aan te moeten stellen.

Artikel 4. Informatie en toegang

De Verordening verplicht de verwerkingsverantwoordelijke om de informatie over de gegevensverwerking eenvoudig toegankelijk en begrijpelijk te maken.

Artikel 5. Categorieën van betrokkenen, doeleinden en persoonsgegevens

Om de Verordening na te leven en te voldoen aan de in de Verordening opgenomen verplichtingen is het van belang om in kaart te brengen welke gegevens van welke personen, met welk doel worden verwerkt en op welke grondslag. Het gaat in dit verband nadrukkelijk om gegevens die onderdeel uitmaken van een bestand als gedefinieerd in dit reglement.

Grondslagen voor het verwerken

Een gegevensverwerking dient in overeenstemming met de wet, behoorlijk en zorgvuldig te geschieden. De persoonsgegevens moeten verzameld zijn voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De verwerking moet een rechtmatige grondslag hebben en mag niet onverenigbaar zijn met het doel waarvoor de werkgever de gegevens heeft verzameld. Artikel 6 lid 1 AVG bevat een opsomming van de enige gronden voor een toelaatbare gegevensverwerking. Met verwerken wordt bedoeld alle handelingen met persoonsgegevens vanaf het verzamelen tot aan het vernietigen. Verstrekken is een vorm van verwerken. De wet kent een limitatief aantal grondslagen op grond waarvan persoonsgegevens mogen worden verwerkt. Deze zijn in de volgorde van artikel 6 lid 1 van de AVG:

Toestemming (artikel 6 lid 1a AVG)

Toestemming is de eerste grondslag op basis waarvan persoonsgegevens mogen worden verwerkt en/of verstrekt aan derden. Deze toestemming kan echter op elk moment worden ingetrokken. Daarmee vervalt de grondslag van de verstrekking en is verwerking van de persoonsgegevens daarna onrechtmatig. Instemming van de Gemeenschappelijke Medezeggenschapsraad voor een bepaalde verstrekking vervangt de individuele toestemming niet.

Het spreekt voor zich dat toestemming vrijwillig moet worden gegeven. Binnen een arbeidsrelatie mag een werkgever echter er niet te snel vanuit gaan dat de werknemer deze toestemming daadwerkelijk vrijwillig heeft gegeven. Geadviseerd wordt om deze grondslag slechts bij uitzondering te gebruiken – wanneer één van de andere grondslagen geen uitkomst kan bieden - en/of in het geval dat uitsluitend de werknemer belang heeft bij verwerking van de gegevens. Denk bijvoorbeeld aan een kortingsactie voor personeel bij de plaatselijke sportschool. Als de verwerkingsverantwoordelijke toestemming vraagt, moet deze duidelijk uitleggen waarvoor de toestemming nodig is en wat de gevolgen zijn van het geven van toestemming.

Voor toestemming gelden drie voorwaarden. De toestemming moet 'vrij' en niet onder druk zijn gegeven. Toestemming moet ondubbelzinnig zijn. Dat betekent dat een school niet uit mag gaan van het principe 'wie zwijgt, stemt toe'. Bij ondubbelzinnige toestemming moet elke twijfel zijn uitgesloten. Het moet dus volstrekt duidelijk zijn óf de betrokkene toestemming heeft gegeven. En de toestemming moet specifiek zijn, voor een specifieke verwerking en voor een specifiek doel. Leerlingen of ouders/voogd moeten hun toestemming ook altijd weer kunnen intrekken.

Verwerkingen waarvoor in ieder geval voorafgaande toestemming is vereist:

1. Foto's en beeldmateriaal van leerlingen

De Autoriteit Persoonsgegevens heeft de onderwijssector op 30 augustus 2017 een brief gestuurd met daarin aanwijzingen met betrekking tot het gebruik van foto's en video's van leerlingen. De AP geeft aan dat zij van mening is dat dit gebruik uitsluitend is toegestaan indien scholen daarvoor toestemming nodig hebben van elke leerling dan wel zijn ouders als de leerling jonger is dan 16 jaar.

2. Diensten van de informatiemaatschappij die rechtstreeks aan de leerling worden aangeboden De AVG verplicht dienstverleners van de informatiemaatschappij om voor deze verwerkingen voorafgaande toestemming te vragen. Voor dit type verwerkingen bepaalt de AVG dat leerlingen die 16 jaar zijn zelf toestemming moet worden gevraagd. Voor leerlingen die jonger zijn dan 16 moet de ouder om toestemming worden gevraagd. Dat laatste geldt ook voor andere verwerkingen echter alleen voor zover die op basis van de toestemmingsgrondslag plaats vinden. Dit volgt niet uit de AVG zelf maar uit de (concept)uitvoeringswet AVG.

Delen van informatie met ouders

Ouders hebben een informatierecht dat is vastgelegd in het BW en in de onderwijswetten.
Informatie die met ouders wordt gedeeld betreft: a. administratieve gegevens;
b. gegevens over onderwijshistorie, leerresultaten en stage- en werkervaring;
c. gegevens over de sociaal-emotionele ontwikkeling en het gedrag;
d. gegevens met betrekking tot de gegeven of geïndiceerde begeleiding;
e. gegevens omtrent de verzuimhistorie.
Dit informatierecht geldt ten aanzien van minderjarige kinderen, die nog niet de leeftijd van 18 jaar hebben bereikt. Omdat de school met het verstrekken van deze informatie uitvoering geeft aan een wettelijke verplichting, is voorafgaande toestemming van de leerling niet nodig, ook niet als deze de leeftijd van 16 jaar nog niet heeft bereikt.

Uitvoeren van een overeenkomst (artikel 6 lid 1b AVG)

Gegevens kunnen worden verstrekt aan derden indien dit noodzakelijk is voor het aangaan van en het uitvoeren van een (arbeids)overeenkomst. Er wordt vanuit gegaan dat ouders, leerlingen en medewerkers bij het sluiten van de overeenkomst zich ervan bewust zijn dat bepaalde gegevens moeten worden verstrekt.
Hoewel de rechtspraak en rechtsliteratuur daarover niet eensluidend zijn, is inmiddels de overheersende opvatting dat het onderwijs tussen leerling/ouders en de school op bijzondere grondslag eveneens op basis van een overeenkomst wordt verstrekt. Over het openbaar onderwijs is de literatuur niet eenduidig.
Omdat voor de meeste gegevensverwerkingen geldt dat deze zijn ingekaderd in wet- en regelgeving en noodzakelijk zijn met het oog op de nakoming van wettelijke verplichtingen dan wel vanwege de uitvoering van een publieke taak, is ervoor gekozen zoveel mogelijk de gegevensverwerkingen te baseren op de op de onderwijsinstelling rustende wettelijke verplichting/publieke taak en – met uitzondering van de inschrijving van de leerling, niet te baseren op de (onderwijs)overeenkomst

Wettelijke verplichting (artikel 6 lid 1c AVG)

De onderwijsinstelling kan verplicht zijn om bepaalde persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van een wettelijke plicht. Ten aanzien van leerlingen zijn deze wettelijke verplichtingen neergelegd in de sectorwetten en de daarop gebaseerde uitvoeringsregelgeving. De onderwijsinstelling is onder andere op grond van artikel 47 van de Algemene wet inzake rijksbelastingen verplicht om de fiscus te voorzien van alle gegevens die van belang kunnen zijn voor de belastingheffing. Ook moet deze op grond van een bevel van de rechter-commissaris in strafzaken verplicht bepaalde persoonsgegevens van een verdacht personeelslid te verstrekken. Ook intern kan de verplichting tot het verwerken van gegevens bestaan, zoals aan de medezeggenschapsraad met het oog op te organiseren verkiezingen of met het oog op het verzorgen van onderwijs, dat eveneens plaats vindt op grond van wettelijke verplichtingen, neergelegd in de Wet op het voortgezet onderwijs en daarop gebaseerde regelgeving.

Vitaal belang (artikel 6 lid 1d AVG)

Deze grond komt niet terug in het reglement, maar kan wel worden gebruikt om gegevens te verstrekken als daarmee een vitaal belang van een leerling of personeelslid is gediend. Gedacht moet worden aan situaties waarin met spoed gehandeld moet worden in het (gezondheids)belang van de betrokkene.

Publiekrechtelijke taak (artikel 6 lid 1e AVG)

Artikel 6, onder lid 1e, maakt gegevensverwerking mogelijk voor zover deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door de school dan wel het bestuursorgaan aan wie de gegevens worden verstrekt.

Gerechtvaardigd belang (artikel 6 lid 1f AVG)

Deze grondslag betreft een restbepaling. In sommige gevallen bestaat de noodzaak voor het behartigen van een gerechtvaardigd belang van de verwerkingsverantwoordelijke en/of derde om

gegevens te verwerken. Het belang op privacy van personeel of leerlingen dient daarvoor dan te wijken. Er dient dan ook steeds een belangenafweging te worden gemaakt waarbij onder meer van belang is wat de aard van de verwerking is, wat voor gegevens er worden verwerkt en hoe deze worden beveiligd. Voor publiekrechtelijke instanties, waartoe in de regel ook het onderwijs wordt gerekend, geldt dat het gerechtvaardigd belang geen grondslag kan vormen voor de kerntaken, omdat daarvoor zou moeten zijn voorzien in een wettelijke grondslag.

Artikel 6. Rechten van betrokkenen

De informatie met betrekking tot dit reglement en de uitvoering ervan die voor de betrokkenen is bestemd moet eenvoudig toegankelijk en begrijpelijk te zijn. De onderwijsinstelling dient op eigen initiatief aan de betrokkenen kenbaar te maken welke verwerkingen van persoonsgegevens hij heeft en waarom. Dit is een belangrijk instrument in de AVG om het gegevensverkeer transparant te maken. Betrokkenen hoeven niet geïnformeerd te worden als hun gegevens worden vastgelegd of verstrekt op grond van een wettelijke plicht. De betrokkene moet op een gemakkelijke wijze zijn rechten op basis van de Verordening en het reglement kunnen uitoefenen. Verzoeken dienen in beginsel kosteloos in behandeling te worden genomen. Betrokkenen dienen middelen te krijgen waarmee verzoeken elektronisch kunnen worden ingediend. Leerlingen van 16 jaar en ouder kunnen zelfstandig hun rechten op grond van de AVG uitoefenen, zoals het recht op inzage in de van hen verwerkte gegevens. Dit recht doorkruist niet het informatierecht van ouders op grond van de onderwijswetten. Scholen zullen ook als de leerling 16 is geworden, ouders nog steeds moeten informeren over de studievoortgang en leerprestaties alsmede over overige zaken die daarop van invloed zijn. Op ouders rust immers een zorgplicht voor hun minderjarige kinderen en zullen daarom in staat moeten worden gesteld aan deze zorgplicht invulling te geven.

Artikel 7. Beveiliging

De AVG verplicht de verwerkingsverantwoordelijke zorg te dragen voor '*een passend beveiligingsniveau*' tegen verlies of tegen enige vorm van onrechtmatige verwerking van persoonsgegevens. De term '*een passend beveiligingsniveau*' geeft in dit verband aan, dat een afweging wordt gemaakt tussen de te leveren beveiligingsinspanning (waaronder ook de kosten!) en de gevoeligheid van de persoonsgegevens. Ook als de verwerkingsverantwoordelijke een verwerker inschakelt voor de verwerking van persoonsgegevens moet hij zorgdragen voor, en toezien op, een afdoende beveiliging van de persoonsgegevens door de verwerker. Dat betreft dan zowel de beveiliging van de apparatuur en programmatuur van de verwerker als de bescherming van de gegevens die door de verschillende communicatienetwerken reizen. Over de beveiliging van persoonsgegevens is meer informatie te vinden op de website van de autoriteit persoonsgegevens.

Stichting Kennisnet ontwikkelt voor de sector PO/VO een normenkader op basis van de ISO-normen, waarin per privacy-norm (afkomstig uit de AVG) of uit de ISO 27001/27002 is beschreven wat scholen ten minste moeten regelen voor een passend beveiligingsniveau. Tot het moment dat dit gereed is, is het advies om gebruik te maken van het normenkader dat is ontwikkeld voor het MBO door saMBO-ICT (bijlage VIII).
Artikel 32 AVG eist dat de onderdelen die betrekking hebben op de bescherming van persoonsgegevens en op de beveiligingsmaatregelen, schriftelijk worden vastgelegd (bijlage VIII).

Artikel 9. Inbreuken op de beveiliging

Voor een uitgebreide toelichting op de wijze van het vaststellen of sprake is van een datalek en of deze gemeld moet worden wordt verwezen naar de voorschriften en werkwijzen die zijn opgenomen in het handboek en protocol Datalekken (bijlage XIII).

Artikel 10. Klachten

Door betrokkenen met een klacht te wijzen op de mogelijkheid tot klachtafwikkeling door de klachtencommissie waarbij de school is aangesloten, kunnen klachten bij de AP voorkomen worden.

Bijlagen behorende bij het Privacyreglement VO-PO

Bijlagenoverzicht

Bijlage I-A Overzicht van toegangsrechten interne verwerkers[1]

Overzicht van diegenen die toegang hebben tot de persoonsregistratie van de Stichting Christelijk Onderwijs Over- en Midden-Betuwe zoals bedoeld in artikel 4 van het Privacyreglement:

Functie	Toegang tot welke persoonsgegevens
Het bestuur	Alle gegevens van het personeel, sollicitanten, leerlingen en hun ouder(s)/verzorger(s), leden van het toezichthoudend orgaan en overig betrokkenen.
(school) directeur/rector	Alle gegevens van personeel werkzaam op de betreffende vestiging, sollicitanten voor op de vestiging vacante posities, alle gegevens van leerlingen en hun ouder(s)/verzorger(s) van de betreffende vestiging.
Functionaris gegevensbescherming	Alle gegevens van het personeel, sollicitanten, leerlingen en hun ouder(s)/verzorger(s), leden van het toezichthoudend orgaan en overige betrokkenen.
Incident Response team (IRT)	Alle gegevens van het personeel, sollicitanten, leerlingen en hun ouder(s)/verzorger(s), leden van het toezichthoudend orgaan en bezoekers.
Medewerkers (centrale) administratie	Alle NAW-gegevens van het personeel, leerlingen en hun ouder(s)/verzorger(s), studieresultaten, aanwezigheidsregistratie, Leerling Volg Systeem hierna LVS.
Medewerkers P&O	Alle gegevens van het personeel en sollicitanten.
Medewerkers financiële administratie	Alle gegevens van het personeel die noodzakelijk zijn voor de uitvoering van de salarisadministratie, of voor de uitbetaling van gemaakte reiskosten van sollicitanten, NAW-gegevens van leerlingen en hun ouder(s)/verzorger(s).
(Preventie)medewerker (P&O)	Gegevens nodig voor het uitvoeren van de wet Poortwachter, NAW-gegevens van het personeel.
(Vestiging) secretariaat	NAW-gegevens van personeel, leerlingen en hun ouder(s)/verzorger(s) van de vestiging, cijfers, aanwezigheidsregistratie, LVS.
Applicatiebeheerder /systeembeheerder/medewerkers ICT/coördinator ICT	Alle gegevens van het personeel, leerlingen en hun ouder(s)/verzorger(s) van de betreffende vestiging, LVS voor zover noodzakelijk voor de uitvoering van de functie.

[1] In het register van verwerkingsactiviteiten aangeduid als een van de 'ontvangers'

Functie	Toegang tot welke persoonsgegevens
School administratie	Alle NAW-gegevens van de leerlingen op de betreffende vestiging.
Decaan/studiecoördinator/mentor	Alle gegevens van leerlingen van de betreffende vestiging met wie ze vanuit hun functie een binding hebben, de NAWgegevens van hun ouder(s)/verzorger(s), LVS.
Docenten/leraren/ groepsleerkrachten	Alle gegevens van de leerlingen van de betreffende vestiging en de ouder(s)/verzorger(s) van de leerlingen aan wie zij lesgeven, cijfers, aanwezigheidsregistratie, LVS.
Intern begeleider (Ib'er)	Alle gegevens van de leerlingen aan wie leraren lesgeven en daarin door de intern begeleider worden ondersteund, cijfers, LVS.
Remedial teacher	Alle gegevens van de leerlingen aan wie de Remedial teacher ondersteuning biedt, cijfers, aanwezigheidsregistratie en LVS.
Medewerker kwaliteitszorg	Toegang tot LVS voor wat betreft gegevens leerlingen ouders en docenten/leraren/groepsleerkrachten.
Leerlingen VO	De NAW-gegevens, behaalde cijfers en aanwezigheidsregistratie van de leerling zelf.
Ouders	De NAW-gegevens, behaalde cijfers en aanwezigheidsregistratie van de eigen kinderen tot de leeftijd van 18 jaar, de eigen persoonsgegevens.
Zorgverleners/zorgteam*	Alle gegevens van de leerlingen van de betreffende vestiging, de NAW-gegevens van de ouders(s)/verzorger(s) en de cijfers, aanwezigheidsregistratie en LVS.
Conciërges	De NAW-gegevens van personeel, leerlingen en ouder(s)/verzorger(s) van de betreffende vestiging, afwezigheidsregistratie.
Teamleiders/onder- en bovenbouwcoördinatoren	De gegevens van leerlingen en ouder(s)/verzorger(s) van de betreffende vestiging, cijfers, aanwezigheidsregistratie en LVS. Alle gegevens van personeel werkzaam op de betreffende vestiging, sollicitanten voor op de vestiging vacante posities.
Examensecretarissen	NAW-gegevens van leerlingen van de betreffende vestiging, NAW-gegevens van hun ouder(s)/verzorger(s), cijfers, aanwezigheidsregistratie, LVS.

Functie	Toegang tot welke persoonsgegevens
Mediatheekmedewerker	Alleen gegevens e-mail en Magister leerlingen van de betreffende vestiging.
Roostermakers	De NAW-gegevens van leerlingen van de betreffende vestiging, aanwezigheidsregistratie. NAW-gegevens medewerkers voorzover noodzakelijk bij roosterinvulling
Verzuim coördinatoren	NAW-gegevens van leerlingen en hun ouder(s)/verzorger(s) van de betreffende vestiging, aanwezigheidsregistratie en LVS.

**Let op: indien externe partijen (arts/schoolbegeleidingsdienst/orthopedagoog) deelnemen aan het zorgteam, dienen met deze partijen aparte afspraken te worden gemaakt.*

NAW-gegevens: een reeks van persoonsgegevens afgeleid van Naam, Adres en Woonplaats welke ook andere gegevens bevat.
LVS: leerlingvolgsysteem voorzover betrekking hebbend op de aangegeven functie.

Bijlage I-B Brondocumenten/brongegevens en bewaartermijnen

Deze bijlage bevat een overzicht van de van de door de verwerkingsverantwoordelijke gehanteerde bewaartermijnen ten aanzien van de brondocumenten en brongegevens die samenhangen met de verwerkingen. De richtlijnen t.a.v. de bewaartermijnen zijn wettelijk. Afwijken mag echter alleen in die gevallen waarbij dat kan worden uitgelegd (pas toe of leg uit). Er is geen verschil tussen digital bewaren en andere wijze van bewaren (op papier, disk etc.). In de kolom “gehanteerde bewaartermijn” is de wettelijke bewaartermijn van 2 jaar als “max. 2 jaar” in de kolom “gehanteerde bewaartermijn”aangegeven aangezien sommige scholen een kortere termijn dan 2 jaar aanhouden. Zie voor verdure uitleg ook de toelichting op pag. 11en 12.

Categorie: leerlingen/oud-leerlingen (onderwijskundig)

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Het onderwijskundig rapport	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	Max. 2 jaar
Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	Max. 2 jaar
Gegevens over leerprestaties van de leerling	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	Max. 2 jaar
Werk van het centraal examen en de rekentoets	minimaal 6 maanden (art. 57 Examenbesluit) Let op: verplichte wettelijke termijn!	na vaststelling van de uitslag	6 maanden tot Max. 2 jaar
Verslagen van gesprekken met de ouders	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	Max. 2 jaar
Psychologisch rapport	maximaal 2 jaar Wanneer het rapport wordt opgevraagd bij een school voor po in het kader van toelating tot een school voor vo minimaal 3 en maximaal 5 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	Max. 2 jaar

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Adresgegevens	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	Max. 2 jaar
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	maximaal 6 maanden (art. 32 lid 6 en art. 34 lid 5 Vrijstellingsbesluit Wbp *oud*)	moment van opname	Max. 6 maanden

Categorie: leerlingen/oud-leerlingen (administratief)

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school ontvangt	minimaal 7 jaar (art. 103a lid 3 Wvo en/of art. 172 lid 3 Wpo) Let op: verplichte wettelijke termijn!	na afloop van het schooljaar waarop de bekostiging betrekking heeft	7 jaar
Gegevens over in– en uitschrijving	minimaal 5 jaar (art. 6 Bekostigingsbesluit Wvo en/of artikel 9 Bekostigingsbesluit Wpo) Let op: verplichte wettelijke termijn!	datum van uitschrijving	5 jaar
Gegevens over verzuim en afwezigheid	minimaal 5 jaar (art. 6 Bekostigingsbesluit Wvo en/of artikel 9 Bekostigingsbesluit Wpo) Let op: verplichte wettelijke termijn!	datum van uitschrijving	5 jaar
Gegevens met betrekking tot de vergoeding van de kosten verbonden aan leerlingvervoer	maximaal 2 jaar (art. 21 lid 5 Vrijstellingsbesluit Wbp *oud*)	na afloop van het schooljaar waarop de verstrekking van de vergoeding betrekking heeft	Max. 2 jaar
Communicatiegegevens oudleerlingen	Verwijderen op verzoek van de leerling of bij diens overlijden (art. 41 lid 5 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving	op verzoek of bij overlijden

Categorie: personeel/oud-medewerkers/leden toezichthoudend orgaan

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Akte van aanstelling/ arbeidsovereenkomst	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Wijzigingen arbeidsovereenkomst	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Correspondentie inzake benoemingen, promotie, demotie	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Aanspraken in verband met de beëindiging van het dienstverband	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	datum waarop aanspraken zijn geëindigd	Max. 2 jaar
Afspraken inzake werk MR	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde lidmaatschap	Max. 2 jaar
Burgerlijke staat werknemer	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Kopie getuigschrift	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Afspraken inzake opleidingen	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Aanvraag opleiding door werknemer	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Afspraken omtrent loopbaan	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Verslagen functionerings- en beoordelingsgesprekken	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Correspondentie UWV en bedrijfsarts	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Verslaglegging inzake Wet Verbetering Poortwachter	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Verzuimregistratie als werkgever eigenrisicodrager Ziektewet is	minimaal 5 jaar De bedrijfsarts moet de gegevens minimaal 10 jaar bewaren. In verband met eigenrisicodragerschap WGA mogen de gegevens voor de duur van het WGA-traject bewaard blijven (10 jaar). (art. 3 lid 2 Regeling werkzaamheden, administratieve voorschriften en kosten eigenrisicodragen ZW) Let op: verplichte wettelijke termijn!	einde dienstverband	5 jaar
Verslaglegging van correspondentie met betrekking tot problematische (financiële) privé-situatie	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Loonbeslagen	tot opheffing (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	-	tot opheffing

Correspondentie met betrekking tot jubilea	tot einde dienstverband (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	-	tot einde dienstverband
Brondocument/brongegevens	**Richtlijn bewaartermijn**	**Ingangsdatum bewaartermijn**	**Gehanteerde bewaartermijn**
Correspondentie directie/PZ/direct leidinggevende	afhankelijk van ontslagsituatie bij einde dienstverband of tot maximaal 2 jaar daarna (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	-	Max. 2 jaar
Identiteitspapieren van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	minimaal 5 jaar (art. 15 lid 4 Wet arbeid vreemdelingen) Let op: verplichte wettelijke termijn!	einde dienstverband	5 jaar
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	maximaal twee jaar (art. 32 lid 6 en art. 34 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	Max. 2 jaar
Loonadministratie	minimaal 7 jaar (art. 52 lid 4 Algemene wet inzake rijksbelastingen) Let op: verplichte wettelijke termijn!	na afloop boekjaar	7 jaar
Loonbelastingverklaringen en kopie identiteitsbewijs uit loonadministratie	minimaal 5 jaar (art. 7.5. lid 4 en art. 7.9. lid 2 Uitvoeringsregeling loonbelasting) Let op: verplichte wettelijke termijn!	na einde kalenderjaar waarin dienstverband is geëindigd	5 jaar
Communicatiegegevens oudpersoneelsleden	Verwijderen op verzoek van het oudpersoneelslid of bij diens overlijden (art. 41 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband	op verzoek of bij overlijden

Categorie: sollicitanten

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn

Sollicitatiebrief, -formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant (art. 5 lid 6 en art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	na beëindiging sollicitatieprocedure of einde dienstverband/benoemings- termijn	maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant

Categorie: leveranciers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Persoonsgegevens van (vertegenwoordigers van) leveranciers	maximaal 2 jaar (art. 13 lid 5 Vrijstellingsbesluit Wbp *oud*)	nadat de desbetreffende transactie is afgewikkeld	Max. 2 jaar

Categorie: huurders

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Persoonsgegevens van huurders	maximaal 2 jaar (art. 14 lid 5 Vrijstellingsbesluit Wbp *oud*)	maximaal 2 jaar nadat de huur is beëindigd	Max. 2 jaar

Categorie: alle bovengenoemde categorieën en bezoekers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn	Gehanteerde bewaartermijn
Camera en videobeelden	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten (art. 38 lid 6 Vrijstellingsbesluit Wbp *oud*)	moment van opname	4 weken dan wel na afhandeling van geconstateerde incidenten
Brondocumenten/brongegevens	**Richtlijn bewaartermijn**	**Ingangsdatum bewaartermijn**	**Gehanteerde bewaartermijn**

Gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de video-opnamen zijn gemaakt.	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten (art. 38 lid 6 Vrijstellingsbesluit Wbp *oud*)	moment van opname	4 weken dan wel na afhandeling van geconstateerde incidenten
Registratielijsten bezoekers	niet langer dan nodig (art. 5 lid 1e AVG)	moment van registratie	niet langer dan nodig

Toelichting ten behoeve van de implementatie van bijlage I-B

Deze bijlage voorziet in een model om bewaartermijnen van de documenten en gegevens in kaart te brengen die samenhangen met de verwerkingen zoals opgenomen in het Register. Het overzicht dient enerzijds als beleidsdocument om werkprocessen binnen de organisatie in overeenstemming te brengen met de verplichting om gegevens (aantoonbaar) niet langer te bewaren dan nodig is. Anderzijds vormt dit overzicht een handzaam document om te kunnen voldoen aan de verplichting om betrokkenen van wie persoonsgegevens worden verwerkt te informeren over de bewaartermijnen die de organisatie hanteert.

Hoofdregel

Volgens de AVG mogen persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor de gegevens zijn verzameld of worden gebruikt (art. 5 lid 1e AVG). Het is dus in beginsel aan de verwerkingsverantwoordelijke om aan de hand van het doel zoals omschreven in het Register van verwerkingsactiviteiten en artikel 5 van het reglement te bepalen hoelang gegevens worden bewaard (de gehanteerde termijnen).

Richtlijn bewaartermijn

Naast de hoofdregel dat persoonsgegevens niet langer mogen worden bewaard dan nodig, heeft de nationale wetgever voor enkele specifieke gegevens en brondocumenten in verschillende wetten al concrete bewaartermijnen gesteld. Deze termijnen zijn in kolom 2 opgenomen als richtlijn voor de te hanteren bewaartermijn. Vaak betreft dit een maximale bewaartermijn, in enkele gevallen schrijft de wet een minimale bewaartermijn voor. Dit betekent voor de verwerkingsverantwoordelijke dat zij ten aanzien van deze documenten naast haar eigen beoordeling, tevens is gebonden aan de minimale en maximale termijnen die uit de wet volgen.

In kolom 2 wordt regelmatig verwezen naar de inmiddels vervallen Wet bescherming persoonsgegevens (Wbp) en het daarbij horende Vrijstellingsbesluit. Hoewel deze wet en dit besluit niet meer van toepassing zijn, zijn de daarin opgenomen concrete bewaartermijnen onverminderd relevant. Bij de totstandkoming van de Wbp en het besluit heeft de wetgever destijds de afweging gemaakt die nu door de verwerkingsverantwoordelijke dient te worden gemaakt; hoelang is het nodig om de gegevens te bewaren met het oog op het doel waarvoor ze worden verzameld? Om deze reden kunnen ook deze inmiddels vervallen wettelijke termijnen dienen als richtlijn om de bewaartermijn vast te stellen. Soms wordt in kolom 2 verwezen naar een bewaartermijn uit een andere wet. Dit betreffen wettelijk termijnen (te herkennen aan: ‘Let op: verplichte wettelijke bewaartermijn!’). Ten aanzien van deze termijnen dient de verwerkingsverantwoordelijk zich ten minste te houden aan de gestelde minimale of maximale termijn uit die wet.

Implementatie

In dit model is reeds het merendeel van de voor het onderwijs relevante persoonsgegevens - gerangschikt naar verschillende typen brondocumenten en brongegevens - opgenomen. Kolom 4 dient te worden aangevuld door de verwerkingsverantwoordelijke, aan de hand van de bewaartermijnen die zij – rekening houdend met de in kolom 2 opgenomen richtlijnen en wettelijke bewaartermijnen – hanteert binnen de eigen organisatie.

Bijlage II Protocol voor het gebruik van e-mail, ICT, en sociale media

Artikel 1 Werkingssfeer van deze regeling, begrippen

1.1 Deze regeling geeft de wijze aan waarop binnen Stichting Christelijk Onderwijs Over- en Midden-Betuwe wordt omgegaan met informatie- en communicatietechnologie (hierna: ICT). Deze regeling omvat (gedrags)regels ten aanzien het gebruik van de ICT en geeft regels voor welke doeleinden en op welke wijze controle plaats vindt op dit gebruik.

1.2 Deze regeling geldt voor eenieder die ten behoeve van de school werkzaamheden verricht (personeelsleden, maar bijvoorbeeld ook: stagiaires en vrijwilligers) of onderwijs volgt (leerlingen). Gezamenlijk worden zij in dit reglement ook aangeduid als 'gebruiker(s)'.

1.3 Elke nieuwe gebruiker wordt gewezen op de toepasselijkheid van deze regeling. Daarbij wordt aangegeven waar de volledige tekst van deze regeling geraadpleegd/ingezien kan worden. Alle personeelsleden en leerlingen ontvangen eens per jaar een herinnering aan de geldende regels.

1.4 Voor zover de gebruikers thuis of elders gebruik maken van de ICT (bijvoorbeeld het emailadres van de school of de schoolwebsite) zijn de bepalingen van deze regeling eveneens van toepassing.

Artikel 2 Toegang tot en gebruik van de ICT

2.1 De Stichting Christelijk Onderwijs Over- en Midden-Betuwe geeft de gebruiker het recht op toegang tot de ICT (en de daarmee verbonden systemen en faciliteiten), maar behoudt zich het recht voor de toegang weer in te trekken.

2.2 Gebruikersidentificatie (gebruikersnaam) en authenticatie (wachtwoord) worden door de ICTafdeling verstrekt en zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.

2.3 Het is gebruiker niet toegestaan om persoonsgegevens die gebruiker ter beschikking staan voor de uitoefening van zijn functie lokaal op te slaan (dus niet op het computernetwerk) noch op privé-apparatuur, tenzij daarvoor voorafgaande toestemming is verleend door diens leidinggevende en adequate waarborgen zijn getroffen voor de beveiliging van de persoonsgegevens.

Artikel 3 Gebruik van de ICT-apparatuur

3.1 De gebruiker dient zorgvuldig om te gaan met de ICT-apparatuur, zodat deze niet beschadigd raakt. De apparatuur dient in goede orde te worden achtergelaten. Eventuele schade of ontbreken van onderdelen dient direct gemeld te worden aan de ICT-afdeling.

3.2 Tijdens het gebruik van de ICT-apparatuur is het niet toegestaan etens- en drinkwaren te nuttigen.

3.3 Alleen de ICT-afdeling is bevoegd om apparatuur te ontkoppelen, verplaatsen of aan te sluiten aan het schoolnetwerk of aan apparatuur die aan het schoolnetwerk verbonden is.

3.4 De ICT-afdeling verleent alleen ondersteuning op apparatuur die door de ICT-afdeling is aangeschaft, aangesloten en geïnstalleerd.

3.5 Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) van de gebruikers is toegestaan, mits onder de volgende voorwaarden:

a) voor het correct laten functioneren van het opslagmedium kan geen beroep worden gedaan op de ICT-afdeling;

b) de bestanden en programmatuur die op het opslagmedium staan moeten voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

3.6 Het gebruik van eigen computerapparatuur (bijvoorbeeld laptops of tablets) is toegestaan onder de volgende voorwaarden:

a) Voorafgaand aan het gebruik is toestemming verleend door de leidinggevende en is contact opgenomen met de ICT-afdeling. Deze is bevoegd om, met opgaaf van redenen, de apparatuur niet toe te staan;

b) de gebruiker geeft de ICT-afdeling de gelegenheid om voorafgaand aan het gebruik maatregelen te treffen om de beheersbaarheid en de veiligheid te waarborgen;

c) het gebruik van de betreffende apparatuur moet voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

Artikel 4 Toegang tot en gebruik van internet en e-mail

4.1 Stichting Christelijk Onderwijs Over- en Midden-Betuwebehoudt zich het recht voor om de toegang tot bepaalde sites door middel van een filtersysteem te beperken.

4.2 Het versturen van e-mailberichten moet voldoen aan de volgende algemene voorwaarden:

a) de afzender wordt correct weergegeven;

b) duidelijke onderwerp aanduiding;

c) terughoudend omgaan met vertrouwelijke gegevens en gevoelige informatie.

4.3 Voor het verzenden en ontvangen van e-mail binnen de school wordt alleen gebruik gemaakt van de e-mailprogrammatuur die de school hiervoor beschikbaar stelt. Het gebruik van andere mailprogrammatuur is niet toegestaan.

4.4 Omdat het verzenden van gegevens met gebruikmaking van Gmail, Hotmail, Dropbox, Whatsapp en WeTransfer leidt, dan wel kan leiden, tot doorgifte van Persoonsgegevens buiten de EER, hetgeen slechts is toegestaan onder voorwaarden, kan Stichting Christelijk Onderwijs Over- en Midden-Betuwe – indien door haar niet langer aan deze voorwaarden kan worden voldaan - besluiten het gebruik van deze software door medewerkers te verbieden.

Artikel 5 (On)verantwoord gebruik van de ICT Verantwoord gebruik

5.1 Het gebruik van de ICT is primair verbonden met taken en bezigheden die voortvloeien uit het verstrekken of ontvangen van onderwijs en begeleiding. Als uitgangspunt geldt dat het gebruik van de ICT van de school ten dienste moet staan aan de werkzaamheden van het

personeelslid of de opleiding van de leerling. Indien en voor zover sprake is van het verwerken van persoonsgegevens gebeurt dit met inachtneming van het Privacyreglement.

5.2 Personeelsleden mogen de ICT beperkt, incidenteel en kortstondig gebruiken voor persoonlijke doeleinden, mits dit niet storend is voor de dagelijkse werkzaamheden of het systeem en mits hierbij wordt voldaan aan de verdere regels van deze regeling. Leerlingen mogen de ICT onder schooltijd in principe niet voor persoonlijke doeleinden gebruiken, tenzij zij daarvoor toestemming hebben gekregen.

5.3 Gebruikers van de ICT systemen melden gesignaleerde zwakke plekken in de systemen, zodat zo snel mogelijk maatregelen kunnen worden getroffen. Melding kan worden gedaan bij de functionaris gegevensbescherming.

Onverantwoord gebruik

5.4 Het is niet toegestaan om de ICT zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast.

5.5 Het is niet toegestaan zich toegang te verschaffen tot gegevens van andere gebruikers, tenzij met uitdrukkelijke toestemming van de betreffende gebruiker.

5.6 Het is niet toegestaan pogingen te ondernemen om het filtersysteem te omzeilen.

5.7 Het is in het bijzonder niet toegestaan om:

a) sites te bezoeken die pornografisch, racistisch, discriminerend, (seksueel) intimiderend, beledigend of aanstootgevend materiaal bevatten;

b) pornografisch, racistisch, discriminerend, (seksueel intimiderend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;

c) zich tot niet-openbare bronnen op het netwerk, internet of andere computernetwerken toegang te verschaffen en het bewust informatie waartoe men via de ICT oneigenlijk toegang heeft verkregen zonder toestemming te veranderen of te vernietigen;

d) bestanden te downloaden en/of op het computernetwerk of lokaal op een PC van de school te plaatsen die geen verband houden met studie en/of werk;

e) software en applicaties te downloaden en/of te installeren zonder voorafgaande toestemming van de ICT-afdeling;

f) niet-educatieve spelletjes te spelen;

g) anoniem of onder een fictieve naam via de ICT te communiceren;

h) op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via de ICT te communiceren;

i) inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;

j) kettingmailberichten en andere berichten die verstopping veroorzaken of het werk van anderen verstoren te verzenden of door te sturen;

k) iemand lastig te vallen via de ICT;

l) het introduceren en verspreiden van computervirussen en andere software die de integriteit van de gegevens of de computerbeveiliging van de ICT kunnen beschadigen;

m) gebruik te maken van social media en andere chatvoorzieningen.

5.8 Het is niet toegestaan om foto's, video's of ander materiaal van op school werkzame personen of leerlingen of andere bij de school betrokkenen via de ICT (daaronder ook begrepen: social media) te publiceren, tenzij dit gericht is op een aan het onderwijs gerelateerde doelstelling en de afgebeelde personen hebben aangegeven in te stemmen met dergelijke publicaties.

5.9 Het is ook anderszins niet toegestaan om door middel van de ICT in strijd met de wet of onethisch te handelen.

5.10 De schoolleiding kan de ICT-afdeling opdracht geven geconstateerde ongeoorloofde data van het computernetwerk te verwijderen.

5.11 Voor personeelsleden is het voor testdoeleinden toegestaan software lokaal te installeren die nodig is voor de werkzaamheden ten behoeve van school.

5.12 Een vermoeden van misbruik van ICT en inbreuken op de beveiliging, van binnenuit of van buiten de school dienen onmiddellijk aan de ICT-afdeling gemeld te worden, hieronder vallen tevens inbreuken op de beveiliging die bij toeval worden ontdekt.

5.13 Als de gebruiker eraan twijfelt of een bepaald gebruik van ICT wel verantwoord is, dan overlegt hij daarover met de ICT-afdeling.

Artikel 6 Algemene uitgangspunten van controle op gebruik

6.1 De schoolleiding heeft er recht op en belang bij dat zij het gebruik van de ICT door personeelsleden en leerlingen kan controleren. De controle op gebruik van de ICT zal overeenkomstig deze regeling uitgevoerd worden. Als zich situaties voordoen waarin deze regeling niet voorziet, dan zal conform de Algemene Verordening Gegevensbescherming (AVG) gehandeld worden.

6.2 Als een directielid merkt of erop geattendeerd wordt dat het ICT-gedrag van een personeelslid niet binnen de kaders van dit reglement verloopt, wordt het personeelslid hierop door het directielid gewezen en wordt een controle van zijn ICT-gebruik door bevoegde personen van de ICT-afdeling als mogelijkheid genoemd. Het directielid meldt dit aan de locatiedirecteur of de centrale directie.

6.3 Als een personeelslid merkt dat het ICT-gedrag van een leerling niet binnen de kaders van dit reglement verloopt, dan spreekt het personeelslid deze leerling hierop aan en meldt dit aan het locatiedirectielid waaronder deze leerling resorteert.

6.4 Gestreefd wordt naar een goede balans tussen enerzijds controle op het gebruik van de ICT en anderzijds de bescherming van de privacy van personeelsleden en leerlingen.

6.5 Controle op het gebruik van de ICT zal waar mogelijk zoveel mogelijk geautomatiseerd plaatsvinden, waarbij in geval van verdachte berichten, het bericht geautomatiseerd wordt teruggezonden aan de verzender. Voor zover geautomatiseerde controle niet mogelijk, dan wel ontoereikend is, zal de controle op het gebruik van de ICT in beginsel steekproefsgewijs plaatsvinden.

6.6 In geval dat ten aanzien van een gebruiker, vanwege een concreet vermoeden van oneigenlijk gebruik, een gerichte controle is uitgevoerd, stelt de schoolleiding deze gebruiker daarvan zo spoedig mogelijk nadat de controle heeft plaatsgevonden van op de hoogte.

6.7 Persoonsgegevens met betrekking tot het gebruik van ICT worden niet langer bewaard dan noodzakelijk, met een bewaartermijn van maximaal 6 maanden. Onder omstandigheden kan een langere bewaartermijn gerechtvaardigd zijn. In dat geval zal de verwerking worden gemeld bij de Autoriteit Persoonsgegevens.

6.8 Privémail/-gebruik (voorzien van het label ‘persoonlijk’) wordt zoveel mogelijk ontzien van controle.

6.9 Elektronische informatie- en communicatieberichten van vertrouwenspersonen en andere personeelsleden met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn uitgesloten van inhoudelijke controle.

6.10 De schoolleiding treft voorzieningen voor de positie en de integriteit van de ICT-afdeling. De medewerkers van de ICT-afdeling hebben een geheimhoudingsplicht die inhoudt dat ten aanzien van de verzamelde en voor hen inzichtelijke informatie strikte geheimhouding betracht dient te worden.

Artikel 7 Doeleinden van controle

7.1 De controle op persoonsgegevens bij gebruik van de ICT vindt slechts plaats met als doel:

a) het tegengaan van onverantwoord en ontoelaatbaar gebruik;
b) de naleving van het Privacyreglement;
c) het bewaken van de voortgang van werkzaamheden;
d) het vastleggen van bewijs en/of archief;
e) de systeem- en netwerkbeveiliging;
f) de kosten- en capaciteitsbeheersing.

7.2 Onder ‘onverantwoord en ontoelaatbaar gebruik’ als bedoeld in artikel 7.1 wordt begrepen: het onverantwoord gebruik als opgenomen in artikel 5.4 tot en met 5.13.

7.3 Onder ‘bewaking van de voortgang van de werkzaamheden’ als bedoeld in artikel 7.1 wordt begrepen: controle op de inhoud van zakelijke e-mails van personeelsleden voor wie het communiceren per e-mail rechtstreeks met de te verrichten taken verband houdt. Middels deze controle kan de voortgang van de werkzaamheden worden gegarandeerd bij ziekte of afwezigheid van de medewerker.

7.4 Onder ‘vastleggen van bewijs en/of archief’ als bedoeld in artikel 7.1 wordt begrepen: het maken van kopieën van e-mails vanuit de behoefte aan bewijs voor zakelijke transacties en dossiervorming (al dan niet met het oog op het voeren van juridische procedures).

7.5 Onder ‘systeem- en netwerkbeveiliging’ als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter voorkoming van systeemaanvallen door onder andere virussen, trojans of andere schadelijke programma’s.

7.6 Onder ‘kosten- en capaciteitsbeheersing’ als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter inventarisering en/of beheersing van de kosten die gemoeid zijn met het gebruik van de ICT.

Artikel 8 Specifieke uitgangspunten van controle op gebruik

8.1 In het kader van de controle op de gebruikers voor het doel als bedoeld in artikel 7.1a geldt dat:

a) controle op de naleving van de regels vindt in beginsel geautomatiseerd en steekproefsgewijs plaats;

b) indien er een concreet vermoeden is dat een gebruiker de regels, waarvan de naleving wordt gecontroleerd, overtreedt, vindt zo nodig een in tijd en omvang zo beperkt mogelijke gerichte controle op persoonsniveau plaats;

c) daarbij worden in eerste instantie de berichten en/of het surfgedrag gescreend op (onder andere) verdachte afzender(s), bestemming, website, verdacht onderwerp, verdachte zoekopdracht, verboden woord in de inhoud of verboden extensies van de bijlage(n);

d) Vervolgens worden de berichten, waarvan aannemelijk is dat het regulier verkeer betreft of waartegen ook overigens geen bedenkingen bestaan, ongeopend doorgezonden (bij originelen) of vernietigd (kopieën);

e) de overgebleven berichten kunnen worden geopend voor nader inhoudelijk onderzoek.

8.2 In het kader van de controle voor het doel als bedoeld in artikel 7.1 b geldt dat slechts berichten worden verwerkt die rechtstreeks verband houden met uitvoering van de te verrichten taken door het personeelslid.

8.3 In het kader van de controle voor het doel als bedoeld in artikel 7.1 c geldt dat slechts de emailverkeersgegevens en inhoud van de berichten wordt verwerkt.

8.4 In het kader van de controle voor het doel als bedoeld in artikel 7.1 d geldt dat slechts zakelijke berichten worden verwerkt voor zover deze kunnen dienen als bewijs van zakelijke transacties en dossiervorming.

8.5 In het kader van de controle voor het doel als bedoeld in artikel 7.1 e geldt dat:

a) de controle geheel geautomatiseerd plaatsvindt;

b) een gevonden besmet bericht/bestand op een aparte locatie bewaard wordt voor nader onderzoek en eventuele herstelwerkzaamheden.

8.6 In het kader van de controle voor het doel als bedoeld in artikel 7.1 e geldt dat slechts de

a) e-mailverkeersgegevens en inhoud (en bijlagen) van berichten met een verdachte inhoud worden gecontroleerd;

b) internetverkeersgegevens en inhoud van berichten met een verdachte inhoud worden gecontroleerd.

8.7 In het kader van de controle voor het doel als bedoeld in artikel 7.1 f geldt dat de controle van het e-mail- en internetverkeer beperkt blijft tot de verkeersgegevens.

8.8 In het kader van de controle voor het doel als bedoeld in artikel 7.1 f geldt dat slechts de

a) e-mailverkeersgegevens over tijd, hoeveelheid, omvang en dergelijke worden verwerkt;

b) internetverkeersgegevens over tijd en dergelijke worden verwerkt.

Artikel 9 Gebruik van social media

9.1 Onder social media wordt verstaan alle huidige en toekomstige online platformen waarbij de gebruikers de inhoud verzorgen.

9.2 Indien social media voor onderwijsdoeleinden worden gebruikt dient dit – met het oog op de bescherming van leerlinggegevens - plaats te vinden conform het Privacyreglement.

9.3 Voor het overig gebruik geldt dat dit in eigen tijd dient plaats te vinden. Dat geldt ook voor het gebruik van social media door middel van smartphones of tablets.

9.4 Voor zover de gebruikers (leerlingen, personeelsleden of derden) aan de school verbonden zijn, geldt in algemene zin dat zich niet op social media zullen uitlaten op een wijze die schadelijk kan zijn voor Stichting Christelijk Onderwijs Over- en Midden-Betuwe.

Artikel 10 Richtlijnen voor het gebruik van social media

10.1 Voor zover de gebruiker op social media-uitingen doet die in relatie staan tot Stichting Christelijk Onderwijs Over- en Midden-Betuwe geeft hij steeds duidelijk aan in welke relatie (bijvoorbeeld: personeelslid of leerling) hij staat tot de school.

10.2 De gebruiker plaatst op social media geen content met een onverantwoorde inhoud.

10.3 De gebruiker deelt op social media geen interne- of bedrijfsvertrouwelijke informatie over de school.

10.4 De gebruiker deelt geen persoonsgegevens van personeel of leerlingen waartoe hij uit hoofde van zijn functie toegang heeft.

10.5 De gebruiker laat zich op social media niet negatief of anderszins ongepast uit over de school, over collega's, over personeelsleden en/of over (mede-)leerlingen.

10.6 De gebruiker plaatst op social media niet zonder toestemming foto's of andere afbeeldingen van de school en/of aan de school verbonden personen.

10.7 De gebruiker plaatst op social media geen content namens de Stichting Christelijk Onderwijs Over- en Midden-Betuwe, tenzij hij daarvoor toestemming heeft gekregen.

10.8 In zijn algemeenheid geldt dat de gebruiker op social media geen content zal plaatsen of zich anderszins zal gedragen op een wijze die de school schade kan toebrengen.

Artikel 11 Richtlijnen voor contact door middel van ICT

11.1 Onderling privé-contact tussen personeelsleden en leerlingen, binnen dan wel buiten schooltijd, door middel van e-mail en smartphones (bijvoorbeeld via Whatsapp) is in beginsel verboden.

11.2 Een uitzondering kan aan de orde zijn ten aanzien van leerlingen die speciale begeleiding op afstand nodig hebben, bijvoorbeeld in geval van ziekte. Een dergelijk contact mag alleen betrekking hebben op onderwijsgerelateerde zaken (bijvoorbeeld kennisoverdracht, afstemming huiswerk, ondersteuning) en dient vooraf gemeld te zijn bij [*wie*]. Het personeelslid mag het contact met de leerling uitsluitend onderhouden via het e-mailadres van de school.

11.3 Onderling contact tussen personeelsleden over een leerling is uitsluitend toegestaan in verband met onderwijsgerelateerde zaken en mag uitsluitend verlopen via het e-mailadres van de school.

11.4 Het is personeelsleden niet toegestaan persoonsgegevens van leerlingen op te slaan op servers die niet worden gebruikt of beheerd door de school of lokaal op de eigen PC respectievelijk tablet of smartphone.

11.5 Gewisselde (e-mail)correspondentie wordt maandelijks door de betrokken docenten vernietigd dan wel – indien de informatie relevant is voor de begeleiding van de leerling - verplaatst en opgeslagen in het leerlingvolgsysteem van de Stichting Christelijk Onderwijs Over- en Midden-Betuwe.

Artikel 12 Disciplinaire maatregelen bij leerlingen

12.1 Indien door de schoolleiding wordt vastgesteld dat een leerling onverantwoord gebruik heeft gemaakt van de ICT, kan de schoolleiding – afhankelijk van de aard en de ernst van het onverantwoorde gebruik – overgaan tot:

a) het tijdelijk uitsluiten van inlogmogelijkheden voor de betrokken leerling;

b) het melden van dit gedrag en de consequenties aan de ouder(s)/verzorger(s); en/of

c) het opleggen van een straf/maatregel.

Artikel 13 Disciplinaire maatregelen bij personeelsleden

Indien door de schoolleiding wordt vastgesteld dat een personeelslid onverantwoord gebruik heeft gemaakt van de ICT, kan de schoolleiding - afhankelijk van de aard en de ernst van het onverantwoorde gebruik – maatregelen treffen, zoals een berisping, schorsing of ontslag.

Bijlage III Protocol gebruik van camera- en videobeelden

Artikel 1 Doel van camera- en video-opnames

Het maken van (digitale)opnames heeft ten doel:

- het zorgdragen voor beveiliging om ongewenst gedrag (waaronder, maar niet uitsluitend: diefstal, vandalisme en pestgedrag) te voorkomen en in voorkomende gevallen te kunnen signaleren en vastleggen.
- het begeleiden en coachen van medewerkers, in het bijzonder maar niet uitsluitend onderwijzend personeel in lessituaties.

Artikel 2 Begripsbepaling

2.1 camera's: het betreft camera's die bedoeld zijn voor algemeen toezicht;

2.2 camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten, glasvezelverbindingen en bevestigingen;

2.3 video-opnames: camera-opnames met als doel begeleiding en coaching van personeel;

2.4 beheer: zorg voor de continuïteit van het cameratoezicht;

2.5 functionaris gegevensbescherming: degene die is belast met het beheer van het camerasysteem;

2.6 beeldinformatie: de door het camerasysteem verkregen en geregistreerde filmbeelden.

Artikel 3 Plaats- en tijdbepaling cameratoezicht en video-opnames

3.1 Cameratoezicht vindt plaats op het schoolterrein van de school (scholen) van Stichting Christelijk Onderwijs Over- en Midden-Betuwe . Binnen de school (scholen) vindt cameratoezicht plaats.

3.2 Video-opnames worden gemaakt in lessituaties, op incidentele basis en steeds vooraangekondigd. Over het moment waarop de opnames worden gemaakt worden de betrokken leerlingen en hun ouders/verzorgers vooraf geïnformeerd.

3.3 Indien een leerling en/of zijn ouders bezwaar hebben tegen de opnames die met het oog op begeleiding en coaching van personeel worden gemaakt, dan zal de school ervoor zorgen dat de leerling tijdens de opnames een dusdanige plek krijgt in de klas dat deze niet in beeld komt.

Artikel 4 Taken, verantwoordelijkheden en beveiliging

4.1 Het cameratoezicht en het maken van video-opnames geschiedt onder verantwoordelijkheid van het College van Bestuur.

4.2 Degene die belast is met het beheer van het camerasysteem is de afdeling ICT .

4.3 Bevoegd tot het bedienen van het camerasysteem en het bekijken van de beelden in de lessituatie is het onderwijzend personeel. Het bekijken van deze beelden kan ook door directieleden gebeuren in het kader van noodzakelijke lesobservaties. De algemene (nietonderwijsbeelden) kunnen worden bekeken door directieleden, conciërges van de betreffende scholen en kunnen worden bediend door de afdeling ICT. Hiervoor is een protocol opgesteld.

4.4 Degenen die toegang hebben tot de camera en videobeelden zullen daarmee strikt vertrouwelijk omgaan. Zij zullen geheimhouding betrachten (zie artikel 4.3. van het Privacyreglement).

4.5 Er zijn passende technische en organisatorische maatregelen getroffen ter beveiliging van de camerabeelden en het camerasysteem.

Artikel 5 Kenbaarheid

5.1 Het cameratoezicht wordt kenbaar gemaakt door middel van borden, stickers op de plaatsen waar cameratoezicht plaatsvindt en bij de ingang van het terrein.

5.2 Video-opnames met als doel begeleiding en coaching worden uitsluitend gemaakt nadat daarvoor uitdrukkelijke toestemming van de betrokken personeelsleden is verkregen en de betrokken leerlingen vooraf zijn geïnformeerd.

5.3 Alle personeelsleden en leerlingen worden geïnformeerd over dit protocol.

5.4 Voor betrokkenen (niet zijnde personeelsleden of leerlingen) ligt het protocol ter inzage d.m.v. intranet en internet.

Artikel 6 Doelbinding, zorgvuldigheid, bewaartermijnen en rechten van betrokkenen

6.1 De geregistreerde camera- en videobeelden worden uitsluitend gebruikt voor de doelstellingen zoals in dit protocol zijn verwoord.

6.2 Het gebruik van de camera- en videobeelden zal niet verder gaan dan strikt noodzakelijk is voor het doel waarvoor het toezicht is ingesteld.

6.3 De camerabeelden die gemaakt zijn met het oog op de veiligheid van de school worden na 4 weken nadat deze zijn gemaakt, verwijderd. De camerabeelden mogen langer bewaard worden in het kader van een wettelijke bewaarplicht of als dat noodzakelijk is voor de afhandeling van geconstateerde incidenten. Zodra het incident is afgehandeld, worden de beelden vernietigd.

6.4 Videobeelden die zijn gemaakt met het oog op begeleiding en coaching van personeel, worden bewaard gedurende het begeleidingstraject. Na afronding van het begeleidingstraject of zoveel eerder als daarom door de medewerker wordt verzocht, worden de beelden vernietigd.

6.5 De betrokkene van wie beelden zijn vastgelegd heeft recht van inzage, recht op rectificatie, recht op wissing en recht op beperking van verwerking van gegevens conform artikel 6 van het Privacyreglement.

Artikel 7 Heimelijk cameratoezicht

7.1 Heimelijk cameratoezicht kan worden ingezet indien er sprake is van een serieus en concreet vermoeden van diefstal, c.q. andere onrechtmatigheden en de Stichting Christelijk Onderwijs Over- en Midden-Betuwe er niet in is geslaagd om met behulp van minder vergaande middelen – waaronder het reguliere cameratoezicht – tot uitkomsten te komen.

7.2 Het heimelijk cameratoezicht wordt in duur en omvang zo beperkt mogelijk gehouden.

7.3 Het heimelijk cameratoezicht zal zich niet uitstrekken tot plaatsen waar de privacy van de betrokkenen onder alle omstandigheden gewaarborgd dient te zijn, waaronder in ieder geval doch niet uitsluitend, de was-en toiletruimten, de kamers van de schoolleiding, de vertrouwenspersoon e.d.

Bijlage IV Geheimhoudingsverklaring

[De heer/mevrouw] [naam], hierna 'medewerker'/functionaris, werkzaam op basis van een akte van benoeming voor de Stichting Christelijk Onderwijs Over- en Midden-Betuwe/een uitzendovereenkomst/ten behoeve van het Zorg Advies Team, hierna 'de Stichting Christelijk Onderwijs Over- en Midden-Betuwe' gevestigd te Bemmel, verklaart zich akkoord met het volgende:

Medewerker heeft uit hoofde van zijn functie toegang tot persoonsgegevens van leerlingen en/of personeel. Medewerker heeft kennisgenomen van het Privacyreglement van de Stichting Christelijk Onderwijs Over- en Midden-Betuwe en de daarin opgenomen voorschriften die gelden bij het verwerken van persoonsgegevens waartoe hij toegang heeft.

1. Het is de medewerker zowel gedurende als na afloop van zijn arbeidsovereenkomst met de Stichting Christelijk Onderwijs Over- en Midden-Betuwe/zijn werkzaamheden voor de Stichting verboden om - ongeacht de wijze waarop en de redenen waarom de arbeidsovereenkomst/de werkzaamheden tot een einde is/zijn gekomen - op enigerlei wijze aan derden, direct of indirect, in welke vorm en op welke wijze dan ook enige mededeling te doen van of aangaande gegevens betreffende de leerlingen en personeel, waarvan de medewerker in het kader van de uitoefening van zijn werkzaamheden voor de Stichting kennis heeft genomen.
2. Deze persoonsgegevens zijn privacygevoelig en mogen uitsluitend worden verwerkt voor het doel waarvoor ze zijn verkregen. De medewerker zal zich bij zijn werkzaamheden ervan vergewissen dat gegevens van leerlingen en personeel uitsluitend worden gedeeld conform het in het Privacyreglement bepaalde.
3. De geheimhoudingsplicht mag worden doorbroken indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de opdracht en de uitvoering van de functie van medewerker of indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.
4. Indien medewerker een (mogelijke) inbreuk op de beveiliging signaleert waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, meldt de medewerker dit per omgaande aan de functionaris gegevensbescherming (FG) ongeacht het tijdstip van de dag. De medewerker is te allen tijde bevoegd zelfstandig een melding te doen bij de voorzitter van het bestuur (telefoonnummer/e-mailadres), dus ook bij het ontbreken van een voorafgaande melding aan de FG.

[Plaats] [datum]:

_____

[naam]

Bijlage V-A Toestemmingsformulier oud-personeelsleden

[Naam school] houdt haar oud-personeelsleden periodiek op de hoogte van nieuws over [naam school] en organiseert voor hen activiteiten en reünies. Als u dit nieuws alsmede uitnodigingen wilt ontvangen voor deze activiteiten en reünies, is het belangrijk dat u [naam school] toestemming geeft om uw persoonlijke gegevens, zoals naam en adres, datum van in- en uitdiensttreding te mogen registreren en te gebruiken voor bovengenoemde doeleinden. Deze kunt u onderaan dit formulier invullen.

In geen geval zal [naam school] uw persoonlijke gegevens delen met derden. Evenmin zal [naam school] uw persoonlijke gegevens gebruiken voor commerciële doeleinden. Mocht u niet langer prijs stellen om van [naam school] informatie of uitnodigingen te ontvangen, dan zal [naam school] uw persoonsgegevens uit de administratie verwijderen.

Meer informatie over hoe wij omgaan met uw persoonsgegevens en uw privacy waarborgen kunt u lezen in onze privacyverklaring (www.sgomb.nl/privacyverklaring). Ook kunt u als u vragen heeft contact opnemen met de Functionaris Gegevensbescherming (FG). De FG op onze school is [naam] en kunt u bereiken via [contactgegevens].

Ja, ik geef [naam school] toestemming om de volgende gegevens van mij te registreren:

Naam: […]
Adres: […]
Woonplaats: […]
Datum van indiensttreding: […]
Datum van uitdiensttreding: […]

[Plaats] [datum]:

_____ (handtekening)
[naam]

Bijlage V-B Toestemmingsformulier oud-leerlingen

[Naam school] houdt haar oud-leerlingen periodiek op de hoogte van nieuws over [naam school] en organiseert voor hen activiteiten en reünies. Als jij dit nieuws alsmede uitnodigingen wilt ontvangen voor deze activiteiten en reünies, is het belangrijk dat jij [naam school] toestemming geeft om jouw persoonlijke gegevens en andere voor de communicatie bedoelde gegevens te mogen verwerken. Deze kun je onderaan dit formulier invullen.

Voor meer informatie over hoe wij omgaan met jouw persoonsgegevens kun je onze privacyverklaring lezen (www.sgomb.nl/privacyverklaring). Ook kun je met vragen terecht bij de Functionaris Gegevensbescherming (FG). De FG op onze school is [naam] en kun je bereiken via [contactgegevens].

Ja, ik geef [naam school] toestemming om de volgende gegevens van mij te registreren:

Naam: […]
Adres: […]
Woonplaats: […]
Datum van inschrijving: […]
Datum verlaten school: […]
Vervolgopleiding (indien van toepassing): […]
Beroep (indien van toepassing): […]

[Plaats] [datum]:

_____
(handtekening van de ouder/verzorger voor leerlingen jonger dan16 jaar)

[naam]

Bijlage VI Privacy statement bezoekers website

Stichting Christelijk Onderwijs Over- en Midden-Betuwe neemt privacy serieus. Indien u wilt weten welke persoonsgegevens wij over u en/of uw kind(eren] hebben vastgelegd, dan kunt u altijd contact opnemen met onze school via de website https://www.sgomb.nl.

In dit privacy statement wordt in het kort beschreven hoe wij met persoonsgegevens van bezoekers van deze website omgaan en deze beveiligen.

Doeleinden van de gegevensverwerking van bezoekers van de website

Als u een contact- of aanmeldformulier op de website invult, of ons een e-mail stuurt, dan worden de gegevens die u ons toestuurt bewaard zolang als naar de aard van het formulier of de inhoud van uw e-mail nodig is voor de volledige beantwoording en afhandeling daarvan.

Klikgedrag en bezoekgegevens

Op de website worden algemene bezoekgegevens bijgehouden. In dit kader kan met name het IPadres van uw computer, de eventuele gebruikersnaam, het tijdstip van opvraging en gegevens die de browser van een bezoeker meestuurt, worden geregistreerd en worden gebruikt voor statistische analyses van bezoek- en klikgedrag op de website. Tevens optimaliseren wij hiermee de werking van de website. Wij proberen deze gegevens zo veel mogelijk te anonimiseren. Deze gegevens worden niet aan derden verstrekt.

Google Analytics[2]

Wij maken gebruik van Google Analytics om bij te houden hoe gebruikers de Website gebruiken en hoe effectief onze Adwords-advertenties bij Google zoekresultaatpagina's zijn. De aldus verkregen informatie wordt, met inbegrip van het adres van uw computer (IP-adres), overgebracht naar en door Google opgeslagen op servers in de Verenigde Staten. Lees het privacybeleid van Google voor meer informatie, alsook het specifieke privacybeleid google analytics.

Google gebruikt deze informatie om bij te houden hoe onze website gebruikt wordt, om rapporten over de Website aan ons te kunnen verstrekken en om haar adverteerders informatie over de effectiviteit van hun campagnes te kunnen bieden. Google kan deze informatie aan derden verschaffen indien Google hiertoe wettelijk wordt verplicht, of voor zover deze derden de informatie namens Google verwerken. Wij hebben hier geen invloed op. Wij hebben Google niet toegestaan de verkregen analytics informatie te gebruiken voor andere Google diensten.

Sociale media

Op deze website zijn knoppen opgenomen om pagina's te kunnen promoten of delen op sociale netwerken [Facebook, LinkedIn, YouTube en Twitter]. Deze knoppen worden gerealiseerd door code die wordt aangeleverd door [Facebook, LinkedIn, YouTube en Twitter] zelf. Deze code plaatst onder meer een cookie (zie boven).

Leest u de privacyverklaring van Facebook, LinkedIn, YouTube en van Twitter (welke regelmatig kunnen wijzigen) om te zien wat zij met uw persoonsgegevens doen die zij met deze code verwerken.

Gebruik van cookies

Wij maken bij het aanbieden van elektronische diensten gebruik van cookies. Een cookie is een eenvoudig klein bestandje dat met pagina's van deze website wordt meegestuurd en door uw

[2] Zie voor het instellen van Google Analytics de handleiding 'Handleiding privacyvriendelijk instellen van Google Analytics' (laatste versie: 6 maart 2018) door de AP via autoriteitspersoonsgegevens.nl.

browser op de harde schijf van uw computer wordt opgeslagen. Wij gebruiken cookies om uw instellingen en voorkeuren te onthouden. U kunt deze cookies uitzetten via uw browser, zie bijvoorbeeld deze toelichting door de Consumentenbond voor uitleg. Ons cookiegebruik is in overeenstemming met de daarvoor geldende regels uit onder meer de Telecommunicatiewet.

Functionele cookies

Om ervoor te zorgen dat onze website goed werkt maken wij gebruik van functionele cookies. Dit zorgt ervoor dat u bijvoorbeeld uw voorkeursinstellingen worden onthouden. Voor het gebruik van deze cookies hebben wij geen toestemming nodig.

Aanpassen privacy statement

Wij behouden ons het recht voor deze privacy statement aan te passen. Wijzigingen zullen op onze website worden gepubliceerd.

Bijlage VII-A Handboek datalekken

Inhoudsopgave

1. Inleiding

Sinds 1 januari 2016 is een verwerkingsverantwoordelijke (in dit verband: de school) verplicht om een datalek te melden aan de Autoriteit persoonsgegevens (AP) en mogelijk ook aan de betrokkenen. Per 25 mei 2018 volgt deze meldingsplicht niet langer uit nationale wetgeving, maar uit de Europese Algemene Verordening Gegevensbescherming (AVG).In dit handboek wordt geregeld hoe het bevoegd gezag dient te handelen indien er (mogelijk) sprake is van een beveiligingsincident aangaande de beveiliging van persoonsgegevens waarvoor de school als verwerkingsverantwoordelijke dient te worden aangemerkt en welke afwegingen zij dient te maken om vast te stellen of daadwerkelijk sprake is van een datalek dat moet worden gemeld aan de AP en/of de betrokkene.

Dit handboek is gebaseerd op het bepaalde in artikel 33 en artikel 34 van de AVG, welke bepalingen als volgt luiden:

Artikel 33 Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

1. *Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.*
2. *De verwerker informeert de verwerkingsverwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.*
3. *In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:*
   a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
   b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
   c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
   d) de maatregelen die de verwerkingsverwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.
4. *Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.*
5. *De verwerkingsverwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.*

Artikel 34 Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

1. *Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.*
2. *De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.*
3. *De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:*
   a) de verwerkingsverwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

b) de verwerkingsverwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer voordoen;

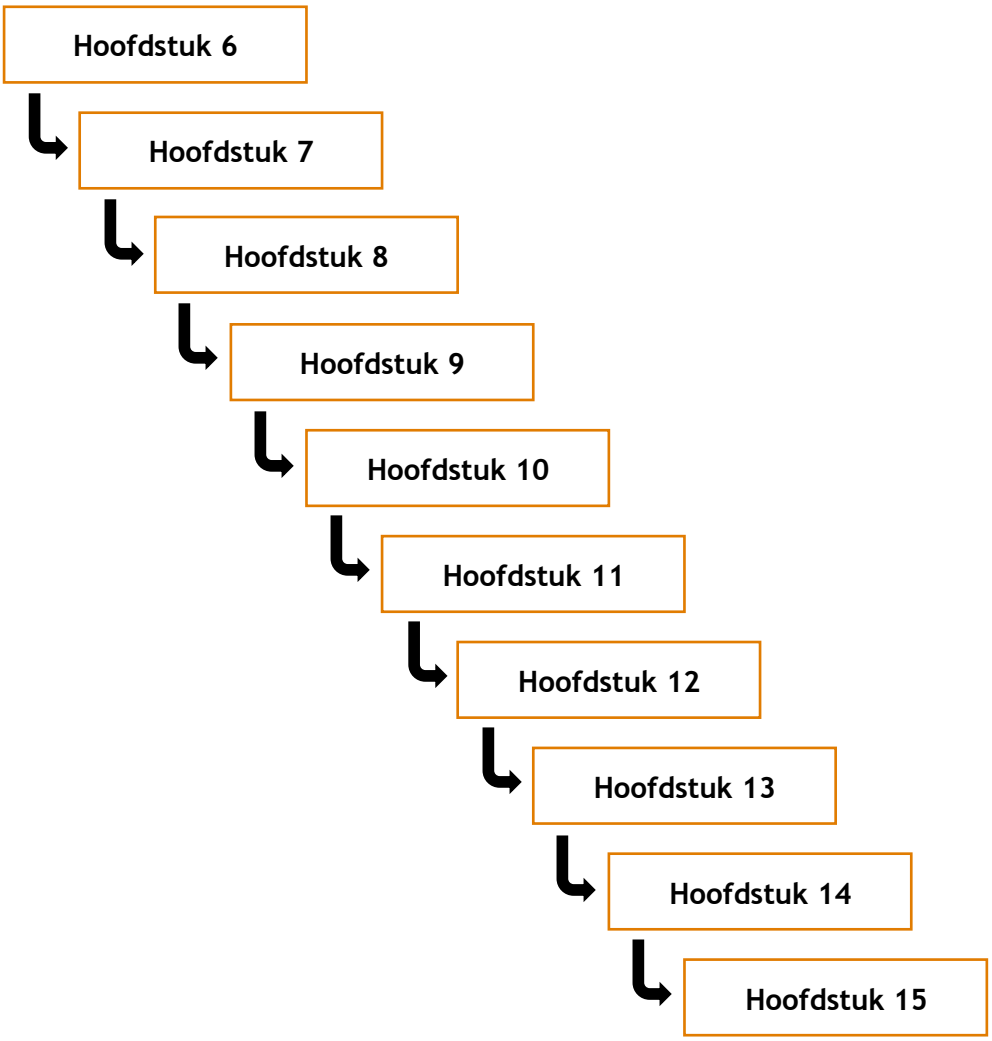
c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

4. *Indien de verwerkingsverwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.*

De inhoud van dit handboek is mede gebaseerd op de nationale Uitvoeringswet AVG en Richtlijnen (guidelines) zoals gepubliceerd door de AP. Tevens is bij dit handboek betrokken hetgeen opgenomen in de Kamerstukken bij wetsvoorstel 33 662, de 'Beleidsregels voor toepassing van artikel 34a van de Wbp' d.d. 8 december 2015. Deze beleidsregels zijn ook na inwerkingtreding van de AVG onverminderd relevant voor de praktische uitwerking van de verplichtingen volgend uit de Verordening.

2. Werkwijze

Dit handboek beschrijft welke stappen de school dient te doorlopen om te kunnen voldoen aan de wettelijke verplichting een datalek – indien noodzakelijk - op de juiste wijze en aan de juiste instanties te melden. Hiertoe is van belang dat indien bij de school/het IRT een signaal binnenkomt dat er mogelijk sprake is van een beveiligingsincident steeds stap voor stap de hoofstukken 6 tot en met 15 doorlopen. Het beginpunt is daarbij steeds hoofdstuk 6 en vervolgens zal op basis van de opvolgende hoofdstukken opgenomen schema's moeten worden vastgesteld of de school/het IRT ook toekomt aan het bepaalde in de opvolgende hoofdstukken.



Van belang is voor een goede werkwijze dat alle besluiten die het IRT/de school neemt op basis van de overwegingen die zij moet maken in het kader van dit handboek schriftelijk en deugdelijk onderbouwd en gemotiveerd vastlegt en bewaard. Dit is onder andere van belang om intern te kunnen monitoren op welke wijze en op basis van welke overwegingen de besluiten zijn genomen.

3. Definities

De onderstaande termen hebben in dit handboek de volgende betekenis:

het bestuur:	vertegenwoordiger van de Stichting Christelijk Onderwijs Over- en Midden-Betuwe;
IRT:	het Incident Response Team van de scholengroep;
FG:	de functionaris gegevensbescherming van de scholengroep (Data Protection Officer);
leerlingen:	de (oud- en/of aspirant)leerlingen van de school;

personeel:	a) de bij de verwerkingsverantwoordelijke benoemde rector, directeur, teamleider/directielid, adjunct-directeur of leraar, en overige medewerkers benoemd in een andere functie dan het geven van onderwijs, waaronder begrepen de leden van het bestuur van die scholen die zijn benoemd door een toezichthoudend orgaan als bedoeld in artikel 24e1, derde lid van de Wet op het Voortgezet Onderwijs, voor zover die leden mede zijn benoemd op basis van een arbeidsovereenkomst of een akte van aanstelling;en b) de onder a bedoelde medewerker die zonder benoeming is tewerkgesteld, tenzij het betreft de toepassing van de artikelen 38a tot en met 39a, 40a, 43a, eerste en tweede lid, 51, eerste tot en met derde lid, 53b en 96o van de wet op het voortgezet onderwijs, voor zover niet anders is bepaald, en de toepassing van daarmee verband houdende wettelijke bepalingen; en betreffende wetsartikelen van de wet op het Primair onderwijs (WPO).
persoonsgegevens:	elk gegeven betreffende een geïdentificeerd of identificeerbare natuurlijke persoon (‘de betrokkene’), waaronder in ieder geval uitdrukkelijk begrepen (de ouder(s) en/of verzorger(s)) van de leerlingen en Medewerkers;
school:	de Stichting Christelijk Onderwijs Over- en Midden-Betuwe vertegenwoordigd door het bestuur;
verwerker:	een partij die (als verwerker) in opdracht – en ten behoeve - van de school persoonsgegevens verwerkt, dan wel een partij die (als subverwerker) op zijn beurt in opdracht van de verwerker voornoemde persoonsgegevens verwerkt;

4. Signaleren van een beveiligingsincident

Medewerkers worden onder andere door middel van het protocol Beveiligingsincidenten (bijlage VII - B) bewust gemaakt onder welke omstandigheden en voorwaarden sprake kan zijn van een beveiligingsincident waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking.

Indien een Medewerker een beveiligingsincident signaleert waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, meldt de Medewerker dit per omgaande aan de FG ongeacht het tijdstip van de dag.

De FG meldt vervolgens op zijn beurt per omgaande het beveiligingsincident telefonisch aan de voorzitter van het bestuur en het hoofd van de ICT-afdeling en bevestigt dit hen per e-mail, tenzij er gegronde redenen zijn om het beveiligingsincident niet per e-mail te bevestigen (bijvoorbeeld indien daarmee duidelijk zou (kunnen) worden voor hackers dat hun hack is ontdekt).

Iedere Medewerker is te allen tijde bevoegd zelfstandig een melding te doen bij de voorzitter van het bestuur (telefoonnummer/e-mailadres), dus ook bij het ontbreken van een voorafgaande melding aan de FG.

Door middel van de melding aan de FG en/of de voorzitter van het bestuur wordt de procedure als verwoord in dit handboek daadwerkelijk gestart.

5. Incident Response Team

Nadat de voorzitter van het bestuur over een (mogelijk) datalek is geïnformeerd, informeert hij op de kortst mogelijke termijn het IRT. De informatie die de voorzitter van het bestuur daarbij verstrekt is de feiten en omstandigheden ten aanzien van het beveiligingsincident en het verzoek paraat te blijven, tenzij de voorzitter van het bestuur van oordeel is dat gegeven de ernst en aard van het beveiligingsincident het IRT direct in overleg dient te treden, in welk geval hij de leden van IRT kenbaar maakt hoe laat het overleg zal plaatsvinden.

IRT bestaat uit de volgende vaste leden:

1) de voorzitter van het College van Bestuur;
2) de FG; en
3) het hoofd van de ICT-afdeling.

Zo nodig wordt het IRT – na een afweging daartoe van de voorzitter van het bestuur - aangevuld met:

4) de forensisch IT-deskundige;
5) de juridisch adviseur; en/of 6) de communicatieadviseur.

De voorzitter van het bestuur is tevens de voorzitter van het IRT en heeft de plicht er voor zorg te dragen dat er steeds een forensisch IT-deskundige, juridisch adviseur en communicatieadviseur beschikbaar zijn en die op de hoogte zijn van hun (mogelijke) rol binnen het IRT. Voorkomen dient derhalve te worden dat de juridisch adviseur en de communicatieadviseur eerst na de melding van een beveiligingsincident dienen te worden aangezocht en aangesteld.

IRT zal opereren vanuit het bezoekadres van het College van Bestuur

De leden van IRT committeren zich om indien zich een beveiligingsincident zich voordoet en zodra zij zijn geïnformeerd door de voorzitter van het IRT om volledig beschikbaar te zijn ten behoeve van het IRT. Besprekingen, overleg en events die een lid van het IRT heeft gepland binnen een tijdsbestek van 96 uur na door de voorzitter van het IRT op de hoogte te zijn gesteld zal het lid annuleren en/of verplaatsen naar een latere datum en tijdstip. Het lid zal zich ook inspannen om zoveel als mogelijk fysiek aanwezig te zijn.

Binnen het IRT hebben slechts de vaste leden stemrecht. Ieder van de vaste leden heeft één stem. Alle besluiten die het IRT neemt worden schriftelijk vastgelegd en voorzien van de afweging die daaraan vooraf is gegaan.

Besluitvorming door het IRT zal plaatsvinden op basis van volledige en juiste informatie aangaande het beveiligingsincident, tenzij gezien de feiten en omstandigheden een besluit – mede met in achtneming van de op basis van de AVG geldende termijnen – niet langer kan worden uitgesteld.

6. Verzamelen volledige en juiste informatie

Nadat de voorzitter van het bestuur over een (mogelijk) beveiligingsincident is geïnformeerd, gaat hij – samen met de FG - tevens direct over tot het verzamelen van de volledige en juiste informatie met

betrekking tot het datalek. Bij het verzamelen van die informatie wordt gebruik gemaakt van het Formulier Gegevens Datalek (bijlage VII-C).

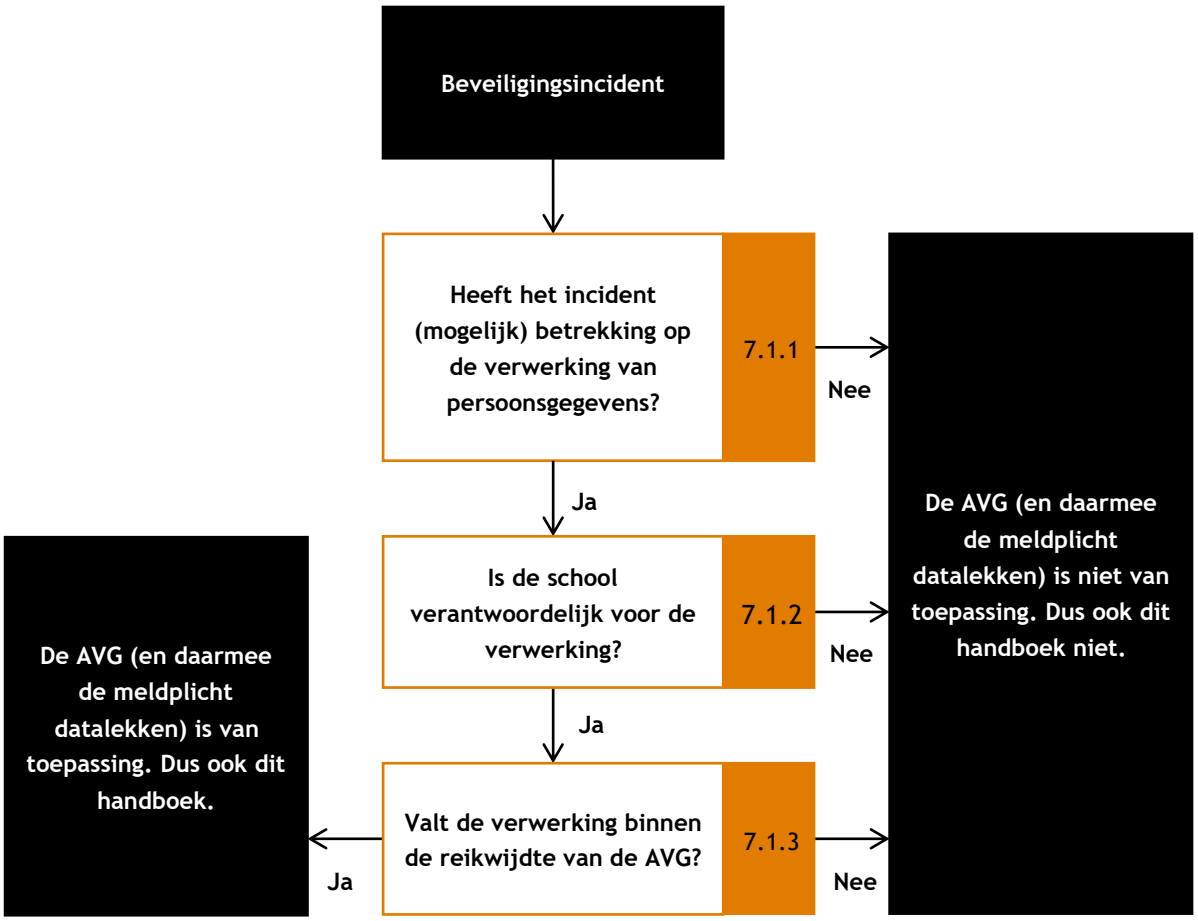
Bij het verzamelen van de benodigde informatie hebben de voorzitter van het bestuur en de FG, althans door hun aangewezen derden - toegang tot alle plekken en ruimtes binnen de school, zijn zij gerechtigd tot inzage in alle informatie, bestanden en/of data die hen geraden voorkomt en kunnen zij met iedereen spreken. Verzoeken tot het verschaffen van informatie die in dit kader (intern) worden gedaan en gegevens die op basis daarvan worden verstrekt, worden schriftelijk gedocumenteerd en liggen ter inzage voor alle leden van het IRT.

7. Is er sprake van een datalek?

Op basis van de verkregen informatie wordt zo snel als mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een datalek. In dit verband dienen feitelijk twee beoordelingen plaats te vinden.

7.1. Eerste beoordeling: is de AVG van toepassing?

De beoordeling of de AVG van toepassing is, vindt plaats op basis van onderstaand schema.



7.1.1. Ziet de melding (mogelijk) op verwerking van persoonsgegevens?

Als er geen sprake is van verwerking van persoonsgegevens, dan zijn de AVG en dit handboek niet van toepassing.

> Voorbeeld 1
> *Indien de school per ongeluk een e-mail verstuurt aan verkeerde personen en in die e-mail enkel melding wordt gemaakt van een toneelstuk dat binnenkort zal worden opgevoerd op school, dan is er geen sprake van verwerking van persoonsgegevens.*

Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene') (artikel 4 lid 1 AVG). Als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd.

Er bestaat een onderscheid tussen direct en indirect identificerende gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum. Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon (bijvoorbeeld: postcode/huisnummer, e-mailadres, kenteken of een leerlingnummer).

Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten (anonimisering).

> Voorbeeld 2
> *Er is geen sprake van verwerking van persoonsgegevens indien een Medewerker een USB-stick verliest met daarop enkel een overzicht van de (gemiddelde) resultaten van een toetsperiode (voor statistieke doeleinden bijvoorbeeld) zonder dat deze resultaten zijn gekoppeld aan een enig ander (direct of indirect) gegeven van de leerling, dan wel leerlingnummer*.

Het toepassen van cryptografische bewerkingen zoals encryptie[3] of hashing[4] op identificerende gegevens leidt tot pseudonimisering (het vervangen van een identificerend gegeven door een ander identificerend gegeven) maar niet tot anonimisering. De school is, ook na de encryptie of hashing, nog steeds in staat om de leerling te identificeren (door bestanden met elkaar te koppelen). Er is dus dan nog steeds sprake van persoonsgegevens. Wel is pseudonimisering een waardevolle beveiligingsmaatregel die bij een datalek de kans op daadwerkelijk misbruik van de gelekte persoonsgegevens aanzienlijk kan verlagen.

Het verwijderen van de direct identificerende gegevens biedt verder niet altijd voldoende garantie dat er geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit een andere bron, kan immers desondanks, soms zonder bijzondere inspanning, identificatie tot stand worden gebracht.

> Voorbeeld 3
> *Indien een Medewerker in de trein een geordende dossiermap laat liggen met daarin de salarisgegevens van de Medewerkers, welke salarisgegevens zijn gekoppeld aan de postcode en huisnummer, is er sprake van verwerking van persoonsgegevens. Zonder bijzondere inspanningen kan via het (digitale) telefoonboek de identiteit van die Medewerkers worden achterhaald*.

Verder moet bij anonimisering rekening worden gehouden met de stand van de techniek. Wat bij een bepaalde stand van de techniek als anoniem kan worden beschouwd, aangezien het gegeven niet

[3] Zie hoofdstuk 11.1
[4] Zie hoofdstuk 11.1

redelijkerwijs tot een persoon te herleiden is, kan door technische ontwikkelingen alsnog een persoonsgegeven worden als gevolg van de toegenomen mogelijkheden tot herleiding.

'Verwerking van persoonsgegevens' betreft elke bewerking of elk geheel van bewerkingen, al dan niet uitgevoerd via geautomatiseerde procedés, met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, structureren, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen, verliezen of vernietigen van gegevens (artikel 4 lid 2 AVG).

7.1.2. Ziet de melding op verwerking van persoonsgegevens waarvoor de school verantwoordelijk is?

De meldplicht datalekken geeft verplichtingen voor de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens. Dit handboek vindt dan ook alleen toepassing indien de school als verwerkingsverantwoordelijke is aan te merken voor de verwerking van de persoonsgegevens (met andere woorden als verwerkingsverantwoordelijke voor het gemelde beveiligingsincident).

De verwerkingsverantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 lid 7 AVG). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking: de vraag op welke manier de gegevensverwerking zal plaatsvinden. Deze bevoegdheden kunnen soms in verschillende handen liggen. In dat geval is er sprake van gezamenlijke verantwoordelijkheid.

De school is in ieder geval als verwerkingsverantwoordelijke aan te merken als het de verwerking van persoonsgegevens betreft aangaande:

- de (ouder(s) en/of verzorger(s)) van de leerlingen van de school; en
- de Medewerkers, en de school ten aanzien van die persoonsgegevens heeft bepaald welke verwerking plaatsvindt en voor welk doel.

Voorbeeld 4

De school is geen verwerkingsverantwoordelijke in het geval een Medewerker een USB-stick zou verliezen met daarop enkel persoonsgegevens van de leden van een sportvereniging (ook al zouden daar leerlingen bij zitten) waarvan de Medewerker bestuurslid is.

Voorbeeld 5

De school is wel verwerkingsverantwoordelijke in het geval een Medewerker een USB-stick zou verliezen met daarop alle voornamen en geboortedatum van de leerlingen op school die de Medewerker hobbymatig bijhoudt om te zien hoe voornamen door de tijd heen veranderen.

7.1.3. Valt de verwerking binnen de reikwijdte van de AVG?

De meldplicht datalekken uit de AVG (en daarmee dit handboek) is uitsluitend van toepassing op verwerkingen waarop de AVG van toepassing is verklaard.

Voor de vraag of de AVG van toepassing is op een verwerking van persoonsgegevens, zijn voor de school feitelijk twee elementen van belang:

- de aard en de doelstelling van de verwerking (artikel 2 AVG)
  Bepaalde verwerkingen vallen door hun aard of hun doelstelling buiten de reikwijdte van de AVG en op deze verwerkingen is de meldplicht datalekken niet van toepassing;

- territoriale reikwijdte: waar vinden de activiteiten plaats waarvoor de persoonsgegevens worden verwerkt, en waar bevinden zich de al dan niet geautomatiseerde middelen die bij de verwerking worden gebruikt (artikel 3 AVG)

Mogelijk is de privacywetgeving van een ander land van toepassing op de verwerking. Ook in deze situaties is de meldplicht datalekken uit de AVG niet van toepassing.

Aard en doelstelling

Voor de school kunnen feitelijk zich maar drie situaties voordoen dat de AVG geen toepassing vindt (en daarmee ook dit handboek niet):

- het betreft persoonsgegevens die door de school niet (geheel of gedeeltelijk) geautomatiseerd zijn verwerkt en die ook niet in een fysiek bestand zijn opgenomen of bedoeld zijn om in een fysiek bestand te worden opgenomen;

> Voorbeeld 6
> *Op school wordt een doos bij het grofvuil gezet met allerhande ongeordende oude brieven en documenten met daarin ook documenten met daarin persoonsgegevens van leerlingen en Medewerkers. Deze fysieke documenten kunnen niet als een bestand worden aangemerkt.*

- het betreft persoonsgegevens die worden verwerkt ten behoeve van activiteiten met uitsluitend persoonlijke doeleinden;

> Voorbeeld 7
> *Een leraar houdt een eigen lijstje bij met de namen van de leerlingen en hun gemiddelde cijfers. Dit lijstje heeft het karakter van persoonlijke aantekeningen, dienend als geheugensteun bij het lesgeven. Dit soort aantekeningen zijn uitgezonderd van de werking van de AVG. Zodra echter beoogd is dit lijstje te worden gebruikt door meerdere personen (bijvoorbeeld: vervangende leraar) is de AVG wel van toepassing.*

- het betreft de verwerking van persoonsgegevens door de school voor uitsluitend journalistieke, artistieke of literaire doeleinden.

> Voorbeeld 8
> *De school verwerkt de vingerafdrukken van een aantal leerlingen met het uitsluitende doel deze te gaan gebruiken voor een kunstwerk dat in de school zal komen te hangen. In dit geval is op deze verwerking de AVG niet van toepassing (en dus ook dit handboek niet).*

7.2. Tweede beoordeling: is er een datalek?

Beveiligingsincident: een inbreuk op de beveiliging die *niet* leidt tot vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens.

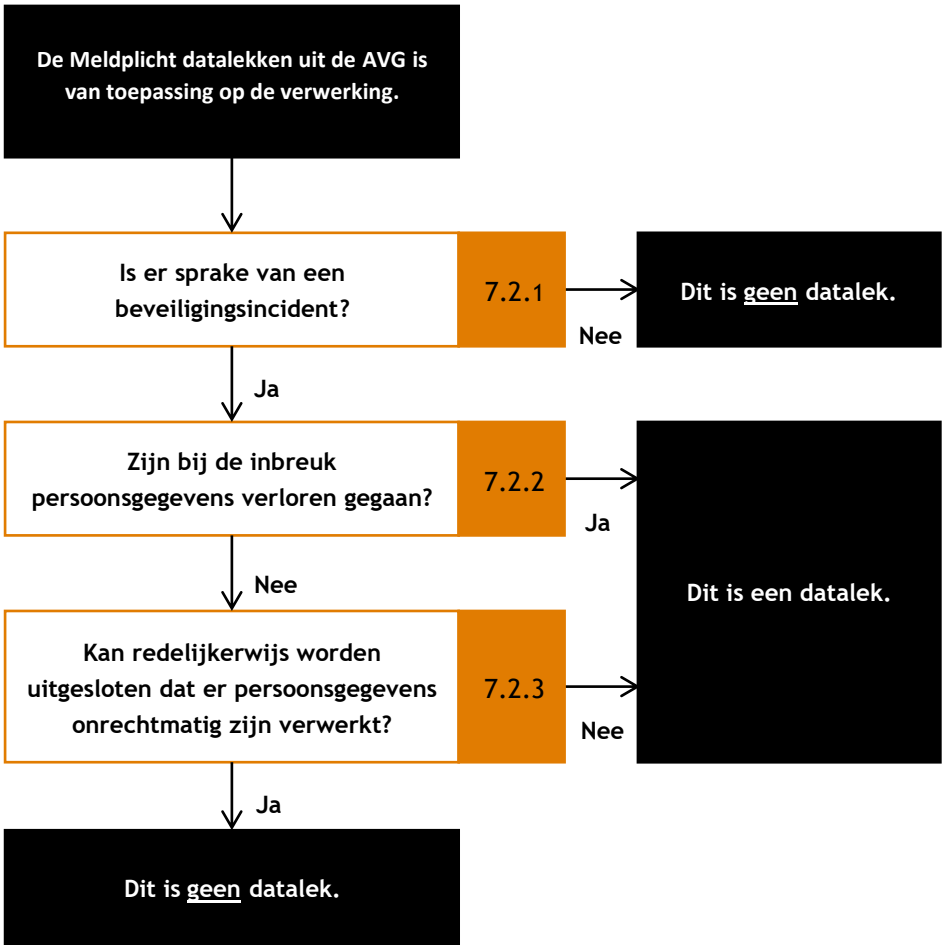
Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens.

In afwijking van hetgeen bepaald is onder hoofdstuk 5 aangaande de besluitvorming zijn de voorzitter van het IRT en de FG gerechtigd gezamenlijk een oordeel te vellen of een melding is aan te merken als een beveiligingsincident of een datalek indien die beoordeling eenvoudig is te maken. Staken in dit kader de stemmen, dan is de stem van de voorzitter van het IRT doorslaggevend. Indien een beoordeling niet eenvoudig lijkt te maken zal het oordeel na overleg met het volledige IRT worden geveld.

De beoordeling of er sprake is van een beveiligingsincident of datalek vindt plaats op basis van onderstaand schema. Het uiteindelijk oordeel wordt altijd schriftelijk onderbouwd, opgeslagen en bewaard.

Ieder datalek moet worden gedocumenteerd, inclusief de feiten omtrent de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. De AP kan deze documentatie opvragen om te controleren of datalekken daadwerkelijk worden gemonitord en opgevolgd.

Om te beschikken over documentatie van ieder datalek dient de school tevens doorlopend goede afspraken te maken met de verwerkers, zodat de school ook over documentatie beschikt van beveiligingsincidenten die hebben plaatsgevonden bij verwerkers. Deze afspraken worden vastgelegd in de verwerkersovereenkomsten die tussen de school en de verwerker worden gesloten. De FG dient zich er steeds van te vergewissen dat bij totstandkoming van een verwerkersovereenkomst afspraken zijn gemaakt over de invulling van de documentatieplicht conform artikel 33 lid 5 AVG, die ook voor de verwerkers geldt.



7.2.1. Is er sprake van een beveiligingsincident?

De school is als verwerkingsverantwoordelijke verplicht om op grond van artikel 32 AVG passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Een beveiligingsincident moet ruim worden uitgelegd. Het betreft alle beveiligingsincidenten waardoor de bescherming van de

persoonsgegevens op enig moment (tijdelijk) is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan mogelijk:

- verlies; of
- onrechtmatige verwerking (inzien, onbevoegde kennisname, wijzigen, verwijderen, doorsturen, etc.).

Het is niet van belang of de school in dit kader al dan niet passende technische of organisatorische maatregelen heeft getroffen (bijv. encryptie). Dat is bij de vaststelling of er sprake is van een inbreuk op de beveiliging niet van belang.

In ieder geval is sprake van een beveiligingsincident waarbij een inbreuk op de beveiliging van de persoonsgegevens plaatsvindt, bij:

- een kwijtgeraakte USB-stick door een Medewerker (al dan niet encrypted);
- een gestolen laptop/mobiele telefoon van een Medewerker (al dan niet encrypted);
- een inbraak door een hacker op het netwerk van de school of van een verwerker;
- een malware-besmetting op het Netwerk van de school of van een verwerker;
- een calamiteit zoals een brand in het datacentrum van de school of van een verwerker;
- het bewust of onbewust prijsgeven door een Medewerker van zijn gebruiksnaam en wachtwoord aan een derde, althans een daartoe onbevoegde derde;
- een toegangsdeur naar een ruimte met personeels- en/of leerlingdossiers die (tijdelijk) niet deugdelijk afgesloten is geweest en daarmee toegankelijk is geweest voor daartoe onbevoegde derden.

7.2.2. Zijn bij het incident persoonsgegevens vernietigd/verloren gegaan?

Verlies van persoonsgegevens houdt in dat de school (of de verwerkers) de persoonsgegevens niet meer hebben; ze zijn weg en niet meer reproduceerbaar. Als gevolg van het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan en de school beschikt niet meer over een complete en actuele reservekopie van de persoonsgegevens. Als er sprake is van vernietiging of verloren gaan van persoonsgegevens is er sprake van een datalek. De aard van het beveiligingsincident is daarbij niet van belang voor het antwoord op de vraag of er sprake is van een datalek. Indien persoonsgegevens verloren gaan als gevolg van bijvoorbeeld brand dan is er sprake van een datalek.

Van vernietiging en het verloren gaan van de persoonsgegevens is in ieder geval sprake indien:

- persoonsgegevens definitief worden verwijderd van de systemen van school en verwerkers als gevolg van een fout van een Medewerker;
- persoonsgegevens vernietigd worden als gevolg van brand in het datacenter van school of verwerker;
- de smartphone of laptop van een Medewerker wordt gestolen en er geen actuele reservekopie beschikbaar is van de gegevens op de smartphone of laptop;
- een Medewerker zijn smartphone of laptop in het water laat vallen en persoonsgegevens op de smartphone of laptop niet meer beschikbaar zijn of kunnen worden gemaakt.

Bovengenoemde omstandigheden kwalificeren echter niet direct als datalek indien van de vernietigde en/of verloren gegane gegevens een actuele reservekopie beschikbaar is voor de school en/of verwerkers.

7.2.3. Valt uit te sluiten dat persoonsgegevens onrechtmatig zijn verwerkt?

Van onrechtmatige verwerking van persoonsgegevens kan in meerdere situaties sprake zijn. Het kan gaan om:

- onbevoegde aantasting van persoonsgegevens;
- onbevoegde wijziging van persoonsgegevens;
- onbevoegde kennisneming van persoonsgegevens;
- onbevoegde doorzending/verstrekking van persoonsgegevens.

Indien de school redelijkerwijs *niet* kan uitsluiten dat de inbreuk op de beveiliging heeft geleid tot een onrechtmatige verwerking, dan moet de school de inbreuk beschouwen als een datalek. Slechts indien uitgesloten kan worden dat de inbreuk op de beveiliging niet heeft geleid tot een onrechtmatige verwerking (en de gegevens zijn niet verloren gegaan), kan de breuk als louter een beveiligingsincident worden aangemerkt.

In geval van een malware-besmetting op het systeem van de school of verwerker moet de school er in ieder geval van uitgaan dat er sprake is van een datalek. Immers, in dat geval kan niet redelijkerwijs worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt.

Voorbeeld 9

Een Medewerker laat zijn laptop onbeheerd achter (in de klas) met daarbij een memo-sticker met daarop zijn inlognaam en wachtwoord. Op de laptop staan alle studieresultaten en leerlingdossiers van een groot aantal leerlingen. Na ontdekking van dit beveiligingsincident past de school/Medewerker direct het wachtwoord van dit account aan. Daarna onderzoekt de school of een derde daadwerkelijk toegang heeft gezocht tot de persoonsgegevens op de laptop. Bij dit onderzoek blijkt uit de logbestanden, waarin per inlognaam is vastgesteld welke acties er op welk tijdstip zijn uitgevoerd met welke gegevens. Uit de loggegevens volgt dat kan worden uitgesloten dat er met de inlognaam toegang is gekregen tot de persoonsgegevens op de laptop gedurende de periode dat het beveiligingsincident zich voordeed. In dat geval is er enkel sprake van een beveiligingsincident en niet van een datalek.

Voorbeeld 10

Een verwerker - ingeschakeld door de school ten behoeve van de salarisadministratie - zendt per ongeluk een bestand met loonstroken van een aantal Medewerkers naar een verkeerd e-mailadres. Zelfs indien de verwerker de ontvanger verzoekt om het bestand (ongelezen) te verwijderen/vernietigen kan de school niet redelijkerwijs uitsluiten dat deze inbreuk heeft geleid tot de situatie dat een onbevoegde kennis heeft genomen van de persoonsgegevens. In dit geval is er sprake van een datalek.

Voorbeeld 11

De toegangsdeur tot een afgesloten ruimte in het schoolgebouw met daarin fysieke leerlingdossiers (die gestructureerd en op alfabet staan opgeslagen) heeft gedurende een bepaalde periode niet op slot gezeten, dan wel heeft zelfs tijdelijk opengestaan. Gedurende deze periode hebben onbevoegden, waaronder leerlingen, de mogelijkheid gehad de leerlingdossiers in te zien. Of dat ook daadwerkelijk het geval is, is niet duidelijk. De school kan echter niet redelijkerwijs uitsluiten dat deze inbreuk heeft geleid tot de situatie dat een onbevoegde kennis heeft genomen van de persoonsgegevens van de leerlingen. In dit geval is er sprake van een datalek.

Als op basis van camerabeelden die op de gang van het schoolgebouw hangen echter kan worden uitgesloten dat gedurende de periode dat het beveiligingsincident zich voordeed er onbevoegden zijn geweest die zich toegang tot de ruimte hebben verschaft, dan kan worden uitgesloten dat er deze inbreuk heeft geleid tot de situatie dat een onbevoegde kennis heeft genomen van de persoonsgegevens van de leerlingen. In dat geval is er geen sprake van een datalek.

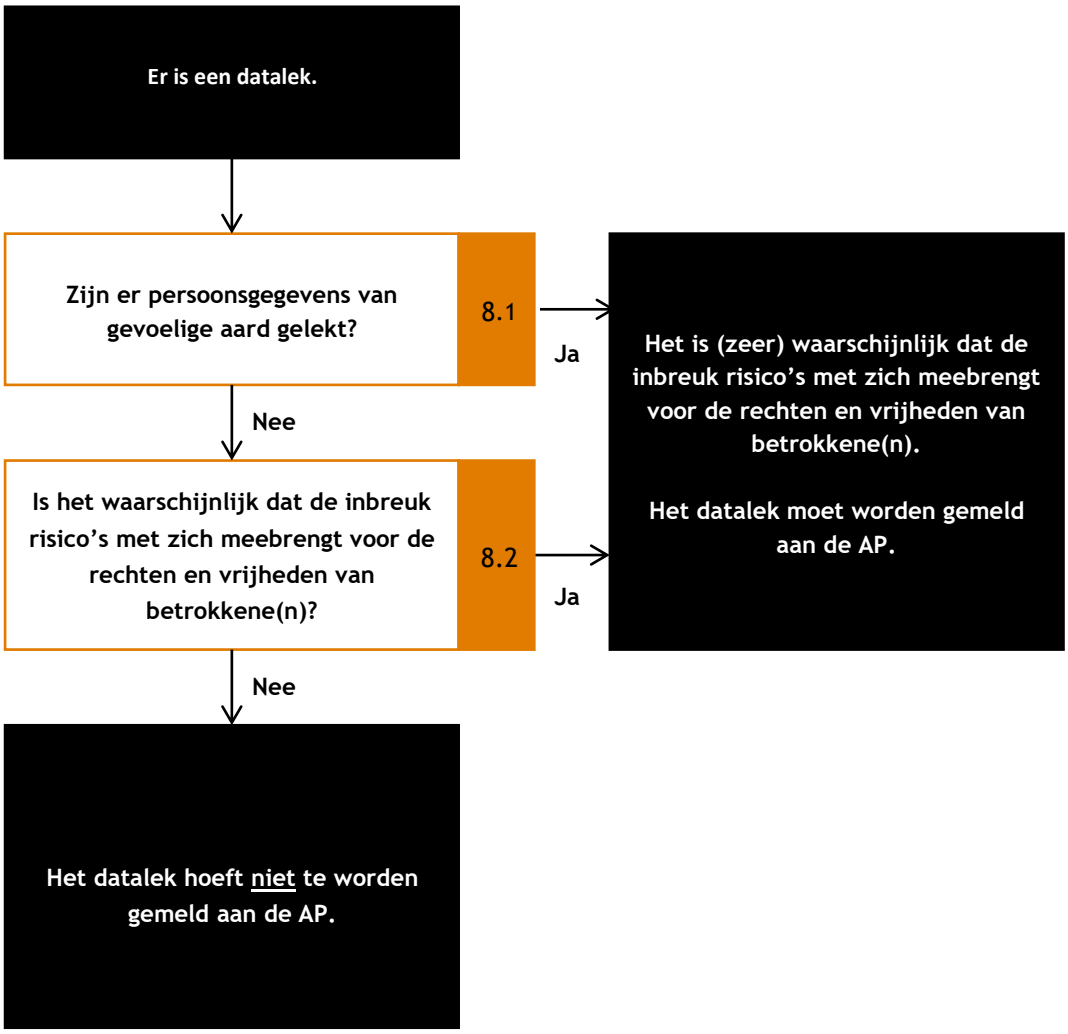
Voorbeeld 12

De adequaat versleutelde laptop van een Medewerker is uit de auto gestolen. Studieresultaten van 1000 leerlingen waren betrokken. Het wachtwoord van de laptop is niet gecompromitteerd en er was een back-up voorhanden, zodat er geen sprake is van een datalek, maar beveiligingsincident.

8. Melding datalek aan Autoriteit persoonsgegevens

Indien wordt geoordeeld door de voorzitter van het IRT en de FG, dan wel het IRT, dat er sprake is van een datalek, dient vervolgens door het IRT bepaald te worden of het datalek aan de AP dient te worden gemeld. De meldingsplicht aan de AP bestaat voor de school alleen indien het datalek leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens.

De beoordeling of melding moet worden gedaan aan de AP en dat het derhalve waarschijnlijk is dat het datalek risico's voor de rechten en vrijheden van natuurlijke personen (betrokkenen) met zich mee heeft gebracht vindt plaats op basis van onderstaand schema.



8.1. Zijn er persoonsgegevens van gevoelige aard gelekt?

Allereerst moet worden gekeken naar de aard van de gegevens die als gevolg van het datalek gelekt zijn. Is er bijvoorbeeld sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn?

Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits)fraude. Tot persoonsgegevens van gevoelige aard moeten in ieder geval worden gerekend:

- *Bijzondere persoonsgegevens zoals bedoeld in artikelen 9 en 10 AVG*

  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras of etnische afkomst, politieke opvattingen, gezondheid, seksuele leven (gedrag en gerichtheid), lidmaatschap van een vakbond, genetische gegevens en biometrische gegevens met het oog op de unieke identificatie van een persoon, strafrechtelijke persoonsgegevens en persoonsgegevens over veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.
- *Gegevens over de financiële of economische situatie van de betrokkene*

Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*

  Hieronder vallen bijvoorbeeld gegevens over prestaties op school, (ontwikkeling van) leergedrag, werk- of relatieproblemen of gokverslaving.[5]

- *Gebruikersnamen, wachtwoorden en andere inloggegevens*

  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude*

  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).

- *Gegevens die onder een beroepsgeheim vallen*

  Het gaat hier bijvoorbeeld om het medisch beroepsgeheim.

Indien derhalve ten aanzien van één of meerdere (ouder(s) en/of verzorger(s) van) leerlingen en/of Medewerkers één of meerdere gegevens van gevoelige aard zijn gelekt, dan dient hoe dan ook gemeld te worden aan de AP.

Voorbeeld 13

Als gevolg van een brand in het datacenter van de verwerker gaan alle studieresultaten van de leerlingen verloren. Er is geen back-up beschikbaar. Er is sprake van het verloren gaan van persoonsgegevens van gevoelige aard.

Voorbeeld 14

Een hacker weet op de website van de school door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een aantal Medewerkers. Normaal gesproken gaat het hier niet om persoonsgegevens van gevoelige aard. Dit wordt anders als deze Medewerkers onderdeel uitmaken van een club binnen de school die zich richt op bijvoorbeeld een specifieke levensovertuiging, politieke voorkeur of seksuele geaardheid.

8.2. Is het waarschijnlijk dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n)?

De aard en omvang van het datalek dient in ogenschouw te worden genomen bij de beantwoording van de vraag of het waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

Een datalek bij grote instellingen zoals de Belastingdienst, de Sociale Verzekeringsbank (SVB), een bank of een verzekeraar kan leiden tot financieel nadeel voor de betrokkene of tot de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht. Datalekken

[5] De AP heeft geoordeeld dat het bij verwerking van persoonsgegevens in het kader van vastlegging van leergedrag kan gaan om zeer gedetailleerde gegevens over de individuele onderwijsvorderingen van een leerling, waaraan allerhande conclusies worden verbonden die mogelijk gevolgen hebben voor het latere maatschappelijke leven van de leerlingen.

in de omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt kunnen ook zeer grote gevolgen hebben voor de betrokkenen.

Verder is het volgende relevant:

- De omvang van de hierboven beschreven verwerkingen betekent dat het bij een datalek kan gaan om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen. Deze beide factoren maken een grote hoeveelheid gelekte data aantrekkelijk voor misbruik in het criminele circuit. De kans dat de gelekte data dan wordt doorverkocht wordt daardoor ook groter, met als gevolg dat de betrokkenen langer last houden van het datalek.
- Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als de school de gegevens gebruikt om het studieadvies van een leerling te bepalen zijn de gevolgen van verlies en onbevoegde wijziging van die gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor het vaststellen van een tussentijdsrapport.
- Bij omvangrijke verwerkingen van de overheid is vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken.

Als de aard en omvang van de getroffen verwerking voldoen aan het bovenstaande, dan moet de school ervan uitgaan dat het waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

Daarnaast kan voor betrokkenen in kwetsbare groepen verlies of onrechtmatige verwerking van persoonsgegevens extra risico's met zich meebrengen. De gevolgen van onbevoegde toegang tot NAW-gegevens zullen bijvoorbeeld voor de meeste betrokkenen beperkt zijn, maar dit ligt anders voor betrokkenen die te maken hebben met bijvoorbeeld stalking of die in een blijf-van-mijn-lijfhuis verblijven. Voor bepaalde categorieën van betrokkenen, zoals kinderen en mensen met een verstandelijke handicap, kan het moeilijker zijn om adequaat om te gaan met de gevolgen van een datalek. Zo zullen zij mogelijk eerder ingaan op pogingen tot phishing of oplichting.

Indien duidelijk is dat gegevens worden verwerkt van betrokkenen in kwetsbare groepen, bijvoorbeeld omdat de verwerking zich specifiek richt op betrokkenen die hiertoe behoren, dan moet ervan worden uitgegaan dat het waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

Dit brengt met zich dat steeds indien er door het datalek persoonsgegevens van leerlingen zijn betrokken (gevoelig van aard of niet) de school ervan uit moet gaan dat het mogelijk waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van deze leerlingen.

Voorbeeld 15

Een hacker weet op de website van de school door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een twintigtal Medewerkers die een nieuwsbrief ontvangen. De nieuwsbrief richt zich op personen die een cursus volgen om vertrouwd te raken met het gebruik van computers en het internet. De aard van de doelgroep leidt hier tot extra risico's voor de betrokkenen.

Gezien de onervarenheid van de betrokkenen met digitale communicatie bestaat er een aanzienlijk risico dat zij in zullen gaan op pogingen tot phishing of oplichting.

Bij een datalek als gevolg van een hack, is van belang wat de aard van de gelekte persoonsgegevens is, en wat de risico's van misbruik van deze persoonsgegevens voor de betrokkene zijn. De intentie bij een hack is veelal kwaadwillend. Bij een hack zal melding dan ook al snel gepast zijn gelet op de risico's van misbruik van persoonsgegevens. Bij een hack ligt ook aangifte bij de politie in de rede in verband met opsporing van de daders.

Indien moet worden vastgesteld dat er geen sprake is van een datalek dat aan de AP dient te worden gemeld, is het ter vrije afweging van het IRT om desondanks de betrokkenen te informeren over het datalek en welke gegevens van hen daar zijn gelekt.

9. Onverwijlde melding aan Autoriteit persoonsgegevens

Indien melding van het datalek aan de AP zal moeten plaatsvinden op grond van de gevoelige aard van de gegevens, dan wel de aard en de omvang daarvan, althans het IRT na zorgvuldige afweging zekerheidshalve tot melding over wenst te gaan aan de AP, dan dient het IRT deze melding *onverwijld* te doen aan de AP.

Het 'onverwijld melden' houdt in dat de school, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. Het betreft hier de tijd benodigd met de stappen als genoemd onder hoofdstukken 6 tot en met 8 van dit handboek. Wat als 'onverwijld' moet worden aangemerkt hangt verder af van de omstandigheden van het geval. Bij een klein en overzichtelijk datalek mag verwacht worden dat sneller na de ontdekking wordt gemeld dan in geval van een omvangrijke hack waarbij langdurig grote hoeveelheden data vanuit verschillende bestanden en servers is gekopieerd.

Onderstaand worden de uitgangspunten opgesomd die de AP met het oog op zijn toezichthoudende en handhavende bevoegdheden hanteert:

- de termijn voor het melden van het datalek begint te lopen op het moment dat de school (als verwerkingsverantwoordelijke), op de hoogte raakt van een beveiligingsincident dat mogelijk onder de meldplicht datalekken valt;
- zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, moet (door de FG) een melding bij de AP worden gedaan, tenzij op dat moment inmiddels al uit het onderzoek van het IRT is gebleken dat het incident niet onder de meldplicht datalekken valt;
- indien het incident later dan 72 uur na ontdekking aan de AP wordt gemeld, dan dient desgevraagd te kunnen worden gemotiveerd aan de AP waarom de melding later heeft plaatsgevonden;
- mogelijk is er 72 uur na de ontdekking van het incident nog niet volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval wordt de melding gedaan op basis van de gegevens waarover op dat moment wordt beschikt. Eventueel kan de melding naderhand nog worden aangevuld of ingetrokken.

Om een datalek tijdig te kunnen melden dient de school steeds doorlopend goede afspraken te maken met de verwerkers, zodat deze de school tijdig en adequaat informeren over alle relevante

beveiligingsincidenten en de school ook de juiste en volledige informatie verschaffen om tijdig de beoordelingen te kunnen maken in het kader van dit handboek. Deze afspraken worden vastgelegd in de verwerkersovereenkomsten die tussen de school en de verwerker worden gesloten. De FG dient zich er steeds van te vergewissen dat bij totstandkoming van een verwerkersovereenkomst is gewaarborgd dat de verwerker verplicht is tijdig een beveiligingsincident te melden en school daarbij te voorzien van de relevante en juiste informatie.

De voorzitter van het IRT is eindverantwoordelijk voor een onverwijlde en tijdige melding aan de AP.

10. Wijze van melding aan Autoriteit persoonsgegevens

Het datalek zal door het IRT worden gemeld bij het AP door middel van het online webformulier zoals dat op de website van de AP (www.autoriteitpersoonsgegevens.nl) beschikbaar is. Een overzicht van de vragen die in dit (web) meldformulier zijn opgenomen zijn als bijlage VII-D van deze bijlagen.

Indien onder omstandigheden – bijvoorbeeld als gevolg van een hack of brand – geen gebruik gemaakt kan worden van het webformulier, dan kan het IRT de gevraagde gegevens per fax (070 - 88 88 501) toezenden aan de AP. Het IRT zorgt daarbij dat kan worden aangetoond dat datum en tijdstip van de melding kan worden aangetoond.

De voorzitter van het IRT is eindverantwoordelijk voor de inhoud van de melding.

In geval een melding aanleiding geeft tot nadere actie door de AP, zal het IRT als contactpersoon functioneren.

11. Melden datalek aan betrokkene?

Na de melding aan de AP dient het IRT te beoordelen of tevens melding dient te worden gedaan bij de betrokkenen bij het datalek. Deze beoordeling maakt het IRT op basis van onderstaand schema.

11.1. Biedt de cryptografie die is toegepast voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten?

Indien passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de persoonsgegevens, dan kan de school de melding aan de betrokkene achterwege laten (artikel 34 lid 3 a AVG).

Cryptografie komt vaak naar voren als het voornaamste voorbeeld van een technische beschermingsmaatregel. Dit onderdeel gaat in op het gebruik van cryptografie als technische

beschermingsmaatregel om persoonsgegevens onbegrijpelijk of ontoegankelijk te maken voor onbevoegden. Andere technische beschermingsmaatregelen worden behandeld in hoofdstuk 11.2.

In dit kader zijn er twee cryptografische bewerkingen:

1) encryptie (versleuteling); en

2) hashing (het omzetten van gegevens in een unieke code). **Encryptie**

Kenmerkend voor encryptie is dat deze bewerking omkeerbaar is: door gebruik van de juiste sleutel kan de oorspronkelijke informatie worden (terug)verkregen (decryptie). Encryptie wordt onder andere toegepast op draagbare hardware (laptops, smartphones) en op verwijderbare media (zoals onder andere USB-sticks) om de gegevens die daarop zijn opgeslagen te beveiligen.

Hashing

Kenmerkend voor hashing is dat het een bewerking betreft die van informatie, ongeacht de lengte, een unieke hashcode maakt die altijd even lang is (de lengte is afhankelijk van de gebruikte hashingmethode). Hashing wordt onder meer gebruikt bij de opslag en verwerking van wachtwoorden: op het moment dat de gebruiker een (nieuw) wachtwoord kiest, wordt de bijbehorende hashcode opgeslagen. Wanneer de gebruiker vervolgens inlogt, wordt de hashcode van het ingevoerde wachtwoord vergeleken met de opgeslagen hashcode en krijgt de gebruiker toegang tot het informatiesysteem als de codes overeenkomen.

Als door de cryptografische bewerkingen die zijn toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege worden gelaten. Dit is een strenge norm, die van geval tot geval moet worden toegepast op basis van de actuele stand van de techniek. Als er twijfel bestaat over de adequaatheid van de technische beschermingsmaatregelen die zijn getroffen, dan moet het datalek gemeld worden aan de betrokkene. In onderstaand schema zijn de beoordelingsgronden opgenomen om tot deze afweging te kunnen komen.

11.1.1. Zijn de persoonsgegevens blootgesteld aan vernietiging of aantasting?

Persoonsgegevens die adequaat zijn versleuteld kunnen bij een datalek nog steeds worden vernietigd, en ook aantasting of onbevoegde wijziging is nog steeds mogelijk (bijvoorbeeld door zogenoemde 'cryptoware', die de reeds versleutelde gegevens nogmaals versleutelt met een sleutel die de school dan uitsluitend tegen betaling in zijn bezit kan krijgen).

Een datalek waarbij adequaat versleutelde persoonsgegevens niet alleen zijn blootgesteld aan onbevoegde kennisname, maar ook aan verlies of aan andere vormen van onrechtmatige verwerking, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan de betrokkene worden gemeld.

Voorbeeld 16

De versleutelde laptop van een Medewerker is gestolen uit de kofferbak van zijn auto. Op de laptop staan de bankrekeningnummers van 200 betrokkenen. Door de diefstal zijn deze gegevens blootgesteld aan onbevoegde kennisname. De school komt tot de conclusie dat alle gegevens op de harde schijf adequaat versleuteld zijn (11.1.3), en dat het restrisico acceptabel is (11.1.4). In principe zou de school de melding aan de betrokkene dus achterwege kunnen laten.
Echter: de school beschikt niet over een back-up (reserve-kopie) van de bankrekeningnummers op de harde schijf. Dat betekent dat er in dit geval niet alleen sprake is van blootstelling aan onbevoegde kennisname, maar ook van het verlies van de getroffen persoonsgegevens. Aangezien de school de gegevens niet meer heeft, zal de school deze opnieuw bij de betrokkenen op moeten vragen. De vertraging die hierdoor ontstaat in de salarisbetalingen, kan tot financiële problemen leiden bij de Medewerkers. In dit geval ligt het, ondanks de genomen technische beschermingsmaatregelen, voor de hand om het datalek te melden aan de betrokkenen. De melding omvat in ieder geval het verzoek om de bankrekeningnummers opnieuw aan te verstrekken en een uitleg van de potentiële consequenties en negatieve gevolgen van de inbreuk.

11.1.2. Waren de persoonsgegevens versleuteld op het moment dat de inbreuk plaatsvond?

Versleuteling beschermt uitsluitend persoonsgegevens die daadwerkelijk versleuteld zijn op het moment dat er een inbreuk plaatsvindt. Een datalek waarbij (ook) niet versleutelde persoonsgegevens zijn gelekt, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk worden gemeld.

Voorbeeld 17

Op de harde schijf van een laptop staat een bestand met persoonsgegevens. Het bestand zelf is niet versleuteld. De laptop wordt automatisch vergrendeld als deze enige tijd niet wordt gebruikt, en bij de automatische vergrendeling wordt de inhoud van de harde schijf versleuteld. De laptop is in handen gekomen van een aanvaller die met technische middelen gebruik van het toetsenbord simuleert, en daardoor voorkomt dat de automatische vergrendeling in werking treedt en de gegevens op de harde schijf worden versleuteld. Er is hier dus geen sprake van een adequate versleuteling en zal gemeld moeten worden aan betrokkenen.

Voorbeeld 18

Een Medewerker geeft aan een derde de gebruikersnaam en het wachtwoord dat toegang geeft tot bepaalde gegevens van alle Medewerkers van de school. Het gaat onder meer om namen, adressen, e-mailadressen, telefoonnummers, toegangs- en andere identificatiegegevens (gebruikersnamen, gehashte wachtwoorden en personeelsnummers) en versleutelde betaalgegevens (waaronder rekeningnummers). Om twee redenen moet de school dit datalek melden aan de betrokkene:

- *slechts een deel van de persoonsgegevens is versleuteld (de wachtwoorden en de betaalgegevens);*
- *de betaalgegevens zijn weliswaar versleuteld opgeslagen, maar als de derde met de verstrekte gegevens inlogt krijgt hij via de gebruikersinterface toegang tot de onversleutelde gegevens.*

11.1.3. Is de versleuteling adequaat?

Het is in eerste instantie aan het IRT om te beoordelen of de versleuteling sterk genoeg is, en op de juiste wijze wordt uitgevoerd.

Zowel encryptie als hashing zijn in principe te 'kraken', wat inhoudt dat onbevoegden toegang kunnen krijgen tot de oorspronkelijke gegevens.[6] Dit terrein ontwikkelt zich voortdurend en het is

[6] Kraken wordt tegengegaan door het gebruik van (combinaties van) moderne cryptografische technieken en door toepassing van zogenoemde salts (extra informatie die bij hashing wordt toegevoegd aan het oorspronkelijke gegeven om het kraken van de hashcode te bemoeilijken). [7] Algemene informatie over algoritmen en toepassingen daarvan zijn te vinden in de publicaties van het European Union Agency for Network and Information Security (ENISA) en het Nationaal Cyber

zeer goed mogelijk dat een cryptografische bewerking die in de huidige situatie veilig genoeg is dat over enige tijd niet meer is. Bij gebruik van cryptografische bewerkingen beoordeelt het IRT daarom periodiek of deze nog steeds voldoende bescherming bieden.

De Europese verordening 611/2013 geeft een nadere invulling aan 'adequate versleuteling'. Volgens deze verordening mogen gegevens als onbegrijpelijk beschouwd worden als ze:

- op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of
- zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.

Aandachtspunten bij de beoordeling zijn:

- Het algoritme zelf, of de wijze waarop deze wordt toegepast, kunnen kwetsbaarheden vertonen waardoor de encryptie of de hashing niet de bescherming biedt die daarvan verwacht mag worden.
- Encryptie is omkeerbaar. Een onbevoegde die over de juiste sleutel beschikt, of deze zonder al te veel moeite kan vinden, kan de gelekte gegevens ontsleutelen.
- Hashing is herhaalbaar. Als bij hashing geen 'salt' is toegepast, of als een onbevoegde over de gebruikte 'salt' beschikt of deze zonder al te veel moeite kan vinden, kan de gebruikte hashingmethode toegepast worden op een lijst met veelgebruikte waarden en daardoor bijvoorbeeld gestolen wachtwoorden worden achterhaald.[7]

Behalve het gebruikte algoritme zelf, is voor adequate versleuteling ook van belang dat dit op de juiste wijze wordt toegepast. Een beoordeling door een deskundige kan hier uitsluitsel over bieden. Bij voorkeur vindt deze beoordeling plaats voordat er een datalek heeft plaatsgevonden zodat, op het moment dat zich een datalek voordoet, gemakkelijk bepaald kan worden of de encryptie of de hashing die is toegepast voldoende bescherming biedt.

Als laatste is van belang dat de gebruikte sleutel c.q. 'salt' niet is gelekt. Dit zal van geval tot geval moeten worden vastgesteld.

11.1.4. Is het restrisico acceptabel?

Door de beantwoording van de voorgaande vragen heeft het IRT, als het goed is, een beeld gekregen van de mate waarin de technische beschermingsmaatregelen die zijn genomen de gelekte

Security Centrum (NCSC). Bij het opstellen van deze beleidsregels was de meest recente publicatie van ENISA op dit gebied het 'Algoritms, key sizes and parameters report – 2014' dat werd gepubliceerd in november 2014.

persoonsgegevens beschermen tegen daadwerkelijke onbevoegde kennisname. Per concreet geval zal moeten worden beoordeeld of de geboden bescherming voldoende is om de kennisgeving aan de betrokkene achterwege te kunnen laten omdat het restrisico beperkt is.

Behalve met wat hierboven is aangegeven, moet het IRT daarbij ook meewegen welke gevolgen het voor de persoonlijke levenssfeer van de betrokkene kan hebben als een aanvaller/onbevoegde er nu of in de toekomst alsnog in slaagt om kennis te nemen van de betrokken persoonsgegevens.

Voorbeeld 19

Een laptop, met op de harde schijf een bestand met persoonsgegevens, is gestolen bij een verwerker. De school als verwerkingsverantwoordelijke onderzoekt het incident, en komt tot de conclusie dat zij op grond van het zesde lid van artikel 34a Wbp af mag zien van de melding aan de betrokkene. Haar overwegingen daarbij zijn:

- *bij de versleuteling van het bestand is gebruik gemaakt van combinatie van algoritme en sleutellengte die door het ENISA in een actuele (niet door een recentere publicatie achterhaalde) handreiking wordt beoordeeld als 'toekomst-vast voor de komende 10 tot 50 jaar;*
- *met betrekking tot het gebruikte algoritme en de implementatie daarvan zijn geen kwetsbaarheden bekend;*
- *de implementatie is met goed gevolg beoordeeld door een deskundige;*
- *het bestand zelf was versleuteld, dus de versleuteling was niet afhankelijk van automatische vergrendeling die in het specifieke geval mogelijk niet heeft gewerkt;*
- *de sleutel is niet gelekt;*
- *gezien de aard van het datalek, de verwerking en de gelekte gegevens is het restrisico acceptabel.*

11.2. Bieden de andere technische beschermingsmaatregelen die zijn genomen voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten?

Remote wipe

Naast encryptie wordt er aangenomen dat er nog een technische beschermingsmaatregel is waarmee persoonsgegevens kunnen worden beschermd tegen onbevoegde kennisname. Het betreft: het op afstand wissen van de gegevens die op hardware staan (*remote wiping*).

Door de gegevens op afstand te wissen zijn deze niet langer beschikbaar voor onbevoegden, aangezien na een geslaagde '*remote wipe*' een onbevoegde nog wel de beschikking heeft over de hardware waarop de gegevens stonden, maar niet meer over de (persoons)gegevens zelf. Een '*remote wipe*' heeft echter uitsluitend kans van slagen als er aan een aantal randvoorwaarden wordt voldaan. Deze luiden als volgt:

- de '*remote wipe*' is tijdig in gang gezet, zodat een onbevoegde nog geen kans heeft gehad om kennis te nemen van de persoonsgegevens;
- de hardware waar het om gaat moet nog intact zijn en werken, zodat het in staat is om de *remote wipe* uit te voeren en de gegevens te wissen;
- de toepassing die voor het wissen van de gegevens wordt gebruikt moet correct werken, zodat alle gegevens waar het om gaat daadwerkelijk worden verwijderd en er ook geen sporen achterblijven waaruit de oorspronkelijke gegevens kunnen worden gereconstrueerd.

Als gebruik gemaakt wordt van '*remote wiping*', dan zal op basis van de specifieke omstandigheden van het geval vastgesteld moeten worden of er wordt voldaan aan de strenge norm van artikel 34 lid 3 a AVG. De voorgaande paragrafen kunnen daarbij gebruikt worden als leidraad bij die vaststelling.

Op voorhand kan wel worden vastgesteld dat de randvoorwaarden zoals gesteld voor een toereikende 'remote wipe' niet altijd met zekerheid zullen kunnen worden vastgesteld door het IRT.

Pseudonimisering

Daarnaast kan er sprake zijn van pseudonimisering. Pseudonimisering wil zeggen dat technische maatregelen zijn genomen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene. Geslaagde pseudonimisering maakt de persoonsgegevens waarover het gaat tot op zekere hoogte onbegrijpelijk voor onbevoegden en de kans dat een datalek daarmee ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene wordt verlaagd. Onvolkomenheden in de wijze waarop de persoonsgegevens zijn gepseudonimiseerd kunnen er echter toe leiden dat onbevoegden de oorspronkelijke identiteit van de betrokkenen alsnog kunnen achterhalen, eventueel met gebruikmaking van andere gegevens die ze reeds in hun bezit hadden of alsnog in hun bezit krijgen.

Ook als de gelekte persoonsgegevens gepseudonimiseerd zijn zal op basis van de specifieke omstandigheden van het geval moeten worden vastgesteld of er aan de norm van artikel 34 lid 3a AVG wordt voldaan.

Net als bij een '*remote wipe'* zult u dus ook bij blootstelling van gepseudonimiseerde gegevens aan onbevoegde kennisname op basis van de specifieke omstandigheden van het geval moeten vaststellen of er wordt voldaan aan de strenge norm van artikel 34a lid 6 Wbp. De onderstaande paragrafen kunt u daarbij gebruiken als leidraad. Verder is aan te bevelen om bij de beoordeling gebruik te maken van het advies over anonimiseringstechnieken dat de samenwerkende Europese toezichthouders in 2014 hebben uitgebracht.

11.3. Houdt het datalek waarschijnlijk een hoog risico in voor de rechten en vrijheden van betrokkene?

Het datalek moet aan de betrokkene worden gemeld indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene (artikel 34 lid 1 AVG).

Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen namelijk onder meer leiden tot onrechtmatige publicatie, aantasting in eer en goede naam, stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, discriminatie, financiële schade of (identiteits)fraude. De schade kan derhalve van materiële en/of van immateriële aard zijn. Het vorenstaande is onder te verdelen in drie onderdelen:

- schending van de vertrouwelijkheid (financiële schade, reputatieschade, chantage, fysieke schade, identiteitsschade, misbruik van inloggegevens);
- beschikbaarheid (bepaalde diensten kunnen niet meer worden verleend, er kan niet (tijdig) betaald worden, betrokkene kan bepaalde activiteiten niet uitoefenen, rechten zoals het recht op verwijdering of rectificatie kunnen niet meer worden uitgeoefend);
- integriteit: (niet langer in overeenstemming met de werkelijkheid: onterechte beslissingen, financiële schade, fysieke schade).

Het is aan het IRT om te beoordelen of een datalek aan de betrokkene wordt gemeld. Indien er echter persoonsgegevens van gevoelige aard zijn gelekt (hoofdstuk 8.1), dan moet het IRT ervan uitgaan dat het datalek - niet alleen aan de AP - maar ook aan de betrokkene moet worden gemeld.

In alle overige gevallen zal op basis van de omstandigheden van het geval een afweging moeten worden gemaakt door het IRT. Daarbij dient het IRT dan ook de aard en omvang van gelekte persoonsgegevens in ogenschouw te nemen (hoofdstuk 8.2). Het IRT stelt zich in dit verband steeds de volgende drie vragen:

- zijn er gevoelige gegevens gelekt?
- houdt de inbreuk waarschijnlijk een hoog risico in voor de rechten en vrijheden van betrokkene?
- hoe groot is het risico dat die nadelige gevolgen ook daadwerkelijk optreden?

Op basis van het antwoord op deze vragen kan het IRT de gevolgen/impact van het datalek voor betrokkene vaststellen op grond van onderstaand schema:[7]

Hoe groot is de impact van het datalek?	Geen gevoelige gegevens gelekt		Wel gevoelige gegevens gelekt	
	Beperkte nadelige gevolgen	Grote nadelige gevolgen	Beperkte nadelige gevolgen	Grote nadelige gevolgen
Kleine kans op nadelige gevolgen	Laag	Gemiddeld	Gemiddeld	Hoog
Grote kans op nadelige gevolgen	Gemiddeld	Hoog	Hoog	Hoog

Het informeren van de betrokkene over een opgetreden datalek is met name noodzakelijk in situaties waarin er voor de betrokkene daadwerkelijk ongunstige gevolgen voor de persoonlijke levenssfeer te duchten zijn (impact: hoog). Door de kennisgeving is de betrokkene alert op de mogelijke gevolgen van het datalek en kan de betrokkene zich, voor zover dat mogelijk is, daartegen beschermen door bijvoorbeeld extra voorzorgsmaatregelen te treffen (zoals vervanging van een wachtwoord) of door bepaalde (software)diensten en/of producten (tijdelijk) niet meer te gebruiken.

De AP kan, indien deze van oordeel is dat de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene, verlangen dat u alsnog een kennisgeving doet (tegen dit besluit staat bezwaar en beroep open).

Voorbeeld 20

Een Medewerker verliest een USB-stick met daarop de ledenlijst van het schoolkoor. Die bevat NAW-gegevens en emailadressen. Dit zijn geen gevoelige gegevens. Als de gegevens in onbevoegde handen vallen, dan kunnen de NAWgegevens misschien gebruikt worden door een rivaliserende schoolkoor, of kan er spam worden verzonden aan de gelekte e-mailadressen. Dat zijn beperkte nadelige gevolgen. De kans op spam is klein vanwege het geringe aantal emailadressen (niet interessant om door te verkopen aan spammers), terwijl ook het scenario van het rivaliserende schoolkoor vrij onwaarschijnlijk lijkt. De te verwachten impact van het datalek is daarmee laag.

[7] Dit schema kan het IRT ook gebruiken om de impact van het datalek op de eigen organisatie vast te stellen. De vragen worden dan gerelateerd aan de school zelf. Op basis van de antwoorden op de vragen, kan dan ook de impact voor de school worden vastgesteld en kan op basis daarvan worden besloten welke mensen en middelen er worden vrijgemaakt en welke acties worden ondernomen. Het gaat dan onder andere om impact als: reputatieschade, staken van proces, verlies van klanten, aansprakelijkheid, boete, intensivering van toezicht en naleving, concurrentienadeel, chantage en misbruik van inloggegevens.

Voorbeeld 21

Hetzelfde voorbeeld, maar nu gaat het om een christelijk koor. In dit geval gaat het om gevoelige persoonsgegevens, omdat ze iets zeggen over de (waarschijnlijke) geloofsovertuiging van de personen op de lijst. Het meest waarschijnlijke nadelige gevolg is dat leden het vervelend vinden dat deze informatie mogelijk naar buiten komt. Dat is een beperkt nadelig gevolg. Bovendien is de kans gering dat het daadwerkelijk optreedt, want waarom zou iemand die deze informatie vindt deze openbaar maken. De te verwachten impact van het datalek is daarmee gemiddeld.

Voorbeeld 22

Hetzelfde voorbeeld, maar nu gaat het niet om een christelijk schoolkoor maar om een schoolvoetbalteam bestaande uit homoseksuele jongens en meisjes. Ook nu gaat het om gevoelige gegevens, en zeker in tijden van homohaat kan het lek grote nadelige gevolgen hebben voor de betrokkenen; denk aan pesterijen of zelfs fysiek geweld. Hoe groot de kans daarop precies is, is dan niet meer relevant: de te verwachten impact van het datalek is hoog.

11.4. Vergt de mededeling onevenredige inspanningen of zou de melding een onderzoek naar de omstandigheden van het datalek nodeloos hinderen?

Onevenredige inspanning

Het IRT mag de melding aan de betrokkene achterwege laten als de mededeling onevenredige inspanningen zou vergen (artikel 34 lid 3c AVG). In dat geval komt in de plaats van de melding aan betrokkene een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd. Van een onevenredige inspanning kan bijvoorbeeld sprake zijn omdat het gaat om een zeer groot aantal betrokkenen of omdat de betrokkenen lastig te contacteren zijn (bijvoorbeeld omdat enkel een IP-adres beschikbaar is). Een openbare mededeling kan bijvoorbeeld zijn een bericht via een regionale of landelijke nieuwswebsite of krant. Een alternatief kan ook meer gerichte communicatie zijn die met grote waarschijnlijkheid alle betrokkenen bereikt. Bijvoorbeeld door een banner of bericht op de schoolwebsite te plaatsen.

Onderzoek naar toedracht

Tot slot zou een reden kunnen zijn om (nog) niet te melden aan de betrokkenen indien dit het onderzoek naar de toedracht van het datalek in gevaar zou kunnen brengen. Het IRT zal dan wel gedegen moeten kunnen onderbouwen waaruit dat gevaar bestaat dat als gemeld wordt aan de betrokkenen de toedracht van het lek niet, of mogelijk niet, achterhaald zal kunnen worden.

12. Hoe melden aan de betrokkene?

De melding aan de betrokkene is steeds schriftelijk en in duidelijke en eenvoudige taal. In de kennisgeving aan de betrokkene wordt in ieder geval vermeld:

- de aard en waarschijnlijke gevolgen van de inbreuk (‘Wat is er aan de hand?’);
- de persoon/instantie waar de betrokkene meer informatie over de inbreuk kan krijgen (‘Waar kan ik terecht met vragen?’);
- de maatregelen die de school heeft voorgesteld of genomen om de inbreuk aan te pakken (‘Wat is er al gedaan’); en
- de maatregelen die de betrokkene worden aanbevolen om de negatieve gevolgen van de inbreuk te beperken (‘Wat kan ik doen?’) (artikel 34 lid 2 AVG).

Bij het beschrijven van de aard van de inbreuk kan de school doorgaans met een algemene omschrijving volstaan. De school neemt de contactgegevens van de FG op zodat de betrokkene hem of haar kan bereiken als de betrokkene vragen heeft over het datalek. Verder geeft de school aan wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken. Te denken valt aan het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn. Het staat de school vrij om meer informatie toe te voegen aan de kennisgeving, maar dit is wettelijk niet verplicht.

Voorbeeld 23

De school biedt haar leerlingen een online account aan waarop ze kunnen inloggen om studieresultaten te raadplegen. De school ontdekt dat een derde zich illegaal toegang heeft verschaft tot de database met gebruikersnamen en wachtwoorden van de website. De wachtwoorden zijn niet adequaat versleuteld. De school onderneemt de volgende acties:

- *zij informeert de (ouder(s) en/of verzorger(s)) van de leerlingen over het datalek. De school raadt daarbij aan om, voor alle accounts (ook die buiten schoolverband) waar de leerling hetzelfde wachtwoord gebruikt, dit wachtwoord te wijzigen;*
- *zij reset alle wachtwoorden en dwingt alle leerlingen om een nieuw wachtwoord op te geven. De school doet dit op een veilige manier zodat zij zeker weet dat het haar leerlingen zijn die een nieuw wachtwoord aanmaken, en niet een onbevoegde derde, en zij geeft hierbij ook aan waarom de leerling een nieuw wachtwoord aan moet maken;*
- *zij past haar systemen aan, zodat alle gebruikte wachtwoorden op een adequate manier worden versleuteld.*

Voorbeeld 24

Mogelijke aanpak als gevolg van datalek op school door 'bug' in software van aanbieder digitaal leermiddel:

- *de school stuurt een e-mail naar de betrokkenen waarin kort wordt aangegeven wat er is gebeurd en wat de betrokkene zelf kan doen om de negatieve gevolgen tegen te gaan.*
- *In de e-mail aan de betrokkenen verwijst de school naar meer uitgebreide informatie op de website van de school. Daar licht de school de aard van de inbreuk en de maatregelen die zijn getroffen en maatregelen die de betrokkene zelf kan treffen waar nodig nader toe.*
- *Verder verwijst de school in de e-mail naar de FG (e-mail, telefoonnummer) waar de betrokkene nadere informatie kan verkrijgen.*

Het belangrijkste is, dat de school zo veel mogelijk betrokkenen bereikt met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaal gesproken niet bereikt. Het IRT dient dan ook zorgvuldig te bepalen via welke kanalen de melding aan de betrokkene wordt gedaan en wat exact aan de betrokkene wordt gemeld. Het IRT zal daar bij voorkeur gebruik maken van de expertise van de communicatiedeskundige.

13. Wanneer melden aan de betrokkene?

De school moet het datalek *onverwijld* melden aan de betrokkene (artikel 34 lid 1 AVG). Onverwijld betekent in dit verband: zonder onredelijke vertraging oftewel zo snel als redelijkerwijs mogelijk. De termijn hangt vooral af van de aard van het risico; hoe acuter het risico hoe sneller de mededeling moet worden gedaan.

Het onverwijld melden houdt in dat, na het ontdekken van het datalek, enige tijd genomen mag worden voor nader onderzoek of het nemen van passende maatregelen zodat de betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd. Voorkomen moet namelijk ook worden dat te snel en daarmee onjuist wordt geïnformeerd richting de betrokkene of dat er te weinig tijd besteed wordt aan het aanpakken van de inbreuk door het nemen van passende maatregelen. Wel moet er rekening mee worden gehouden dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de school de betrokkene daarover informeert, hoe eerder deze in actie kan komen.

Net als bij de melding aan de AP kan er eventueel voor gekozen worden door het IRT om de betrokkene in eerste instantie te informeren op basis van de informatie waarover op dat moment wordt beschikt, zodat de betrokkene alvast maatregelen kan gaan treffen om zich te beschermen tegen de gevolgen van het datalek, en om deze informatie in tweede instantie op basis van nader onderzoek aan te vullen.

Voorbeeld 25

Indien de school weet dat onbevoegden toegang hebben gehad tot een database met inloggegevens, maar dat de school nog aan het onderzoeken is of de onbevoegden ook andere persoonsgegevens hebben ingezien, kan de school in een dergelijk geval meteen al beginnen met het resetten van de getroffen wachtwoorden en met het informeren van de betrokkenen, waarbij zij aangeeft dat betrokkenen, als zij elders dezelfde inloggegevens gebruiken, deze moeten wijzigen.

In de melding aan de AP moet worden aangeven of het datalek al aan de betrokkenen is gemeld en, zo niet, wanneer dat dan wel plaatsvindt. De termijn die in de melding aan de AP wordt aangegeven, moet ook worden nagekomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan dient dat tijdig aan de AP te worden kenbaar gemaakt door middel van een aanpassing van de melding.

14. Melden aan overige partijen

Melding aan de AP en betrokkene zijn verplicht op basis van artikel 33 en artikel 34 AVG, althans als op basis voor vorenstaande hoofdstukken is geoordeeld dat melding verplicht is. Dat neemt niet weg dat het voor de school noodzakelijk kan zijn om ook andere partijen – binnen en buiten de school – te informeren. Te denken valt aan partijen als:

- de verzekeraar van de school;
- Medewerkers (indien zij geen betrokkenen zijn); • brancheorganisaties/ketenpartners (verwerkers); en
- media.

Van belang is dat de school probeert de communicatie met betrekking tot het datalek zo veel mogelijk in eigen hand te houden (ook intern). In dat verband is ook het IRT als enige binnen de school gerechtigd naar buiten toe te communiceren over het datalek. Daarmee wordt bereikt dat de school zelf deze derden kan berichten in plaats van dat zij dat van anderen (of zelfs vanuit de media) moeten vernemen. Hierdoor wordt ook bewerkstelligd dat er feitelijke gegevens over het datalek openbaar worden gemaakt in plaats van speculaties en mogelijk ‘spookverhalen’.

Melding aan overige partijen wordt niet in de AVG voorgeschreven, maar indien wel besloten wordt te melden aan overige partijen kan het IRT daarbij het meest geschikte moment kiezen. Er zijn immers geen termijnen die in dit kader gelden. Het IRT kan dan ook namens de school communiceren met de overige partijen op het moment – en de wijze – waarop het best uitkomt voor de school. Het IRT zal – indien communicatie aan derden wenselijk/noodzakelijk is - een communicatieplan en actieplan opstellen voor deze eerste communicatie over het datalek, welk plan in ieder geval mede wordt afgestemd op de communicatie aan de betrokkene en AP. Bij het opstellen van een communicatieplan zal dan bij voorkeur de communicatieadviseur een belangrijke rol spelen.

De school zal in haar verwerkersovereenkomsten met verwerkers op voorhand afspraken maken dat de school beslist wie, wanneer en hoe het datalek extern (dus aan andere partijen dan AP en

betrokkenen) wordt gecommuniceerd. Op deze wijze heeft de school de externe communicatie met betrekking tot het datalek in de hand en kan zij er ook voor kiezen welke partij (op positieve of negatieve wijze) op de voorgrond treedt. Zo zou een overweging kunnen zijn om de communicatie aan de derden door de verwerker te laten doen waar het datalek is ontstaan om zo de reputatieschade voor de school te beperken.

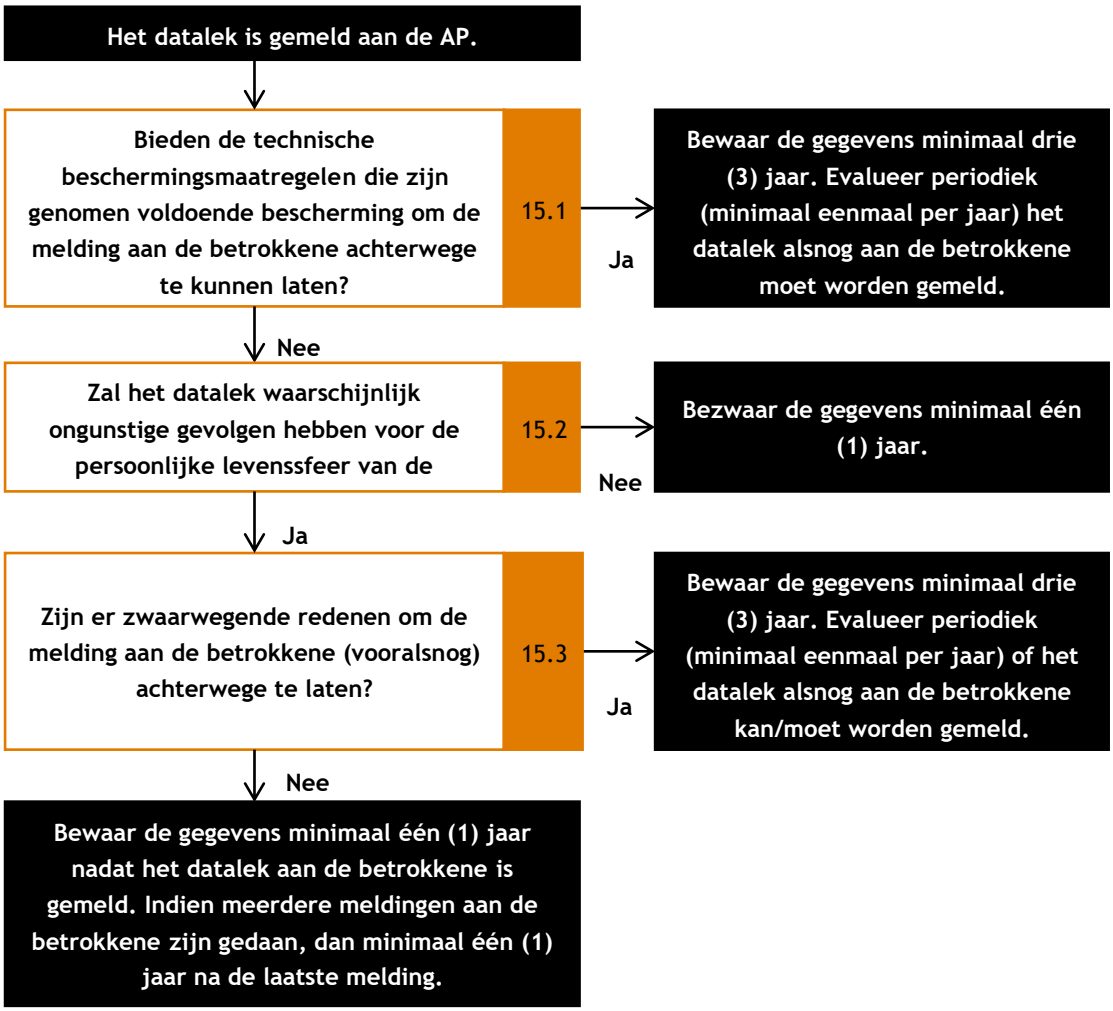
15. Welke gegevens moet de school documenteren?

De school dient ieder beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of ongeoorloofd zijn gewijzigd, verstrekt of ingezien, ongeacht of het moet worden gemeld, te documenteren (art. 33 lid 5 AVG), zie bijlage VII-E. Het overzicht hoeft niet openbaar te worden gemaakt. Per beveiligingsincident bevat het overzicht in ieder geval:

- de feiten en gegevens omtrent de aard van de inbreuk; en
- een beschrijving van de gevolgen van de inbreuk en de genomen corrigerende maatregelen.

De AP kan toegang verlangen tot deze documentatie en de documentatie moet adequaat zijn om de toezichthouder te laten controleren of beveiligingsincidenten daadwerkelijk worden gemonitord en opgevolgd. Zoals reeds aan bod is gekomen in paragraaf 7.2. betekent deze verplichting dat de school in een verwerkersovereenkomst duidelijke afspraken moet maken met verwerkers over de wijze van documenteren ten aanzien van beveiligingsincidenten die zich (mogelijk) voordoen bij verwerkers.

Wettelijk is niet voorgeschreven voor hoelang het overzicht moet worden bewaard. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren. Het onderstaande schema biedt u een beslismodel voor het vaststellen van de bewaartermijnen van geregistreerde datalekken zoals opgesteld in de beleidsregels van de AP.



Het bovenstaande schema gaat ervan uit dat de school de gegevens voor de volgende doeleinden bewaart:

- lering trekken uit het datalek en uit de wijze waarop het IRT dit heeft afgehandeld;
- antwoord kunnen geven op vragen van betrokkenen en derden;
- alsnog melden van het datalek aan de betrokkenen, indien dit in eerste instantie achterwege is gelaten en de omstandigheden vereisen dat dit alsnog gebeurt.

Voorbeeld 27

Het laatste bullet point kan zich voordoen als de school bij diefstal van een versleutelde USB-stick besluit om de kennisgeving aan de betrokkene achterwege te laten. De school moet zich er in een dergelijke situatie van bewust zijn dat de komst van nieuwe technieken nieuwe risico's kan inhouden, en dat er met grote regelmaat nieuwe kwetsbaarheden in breed gebruikte versleutelingsalgoritmen worden ontdekt. Dit houdt in dat de school, met de diefstal van de versleutelde USB-stick in het achterhoofd, over een langere periode alert moet zijn op deze risico's. Bij signalen van mogelijke 'ontsleuteling' zal de school alsnog de afweging moeten maken of u de betrokken personen moet informeren.

Er dient verder rekening mee gehouden te worden dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat de school waar dat aan de

orde is het bewijsmateriaal moet verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Nadat zich binnen de school een datalek heeft voorgedaan dat is gemeld aan de AP, zal de FG ieder half jaar een vergadering beleggen waarbij de vaste leden van het IRT bij aanwezig zullen zijn. Indien daar aanleiding voor is kunnen daarvoor door de FG – in overleg met de voorzitter van het IRT - ook de forensisch IT-deskundige, juridisch adviseur of communicatieadviseur voor worden uitgenodigd. Tijdens deze bespreking stelt het IRT vast of er met betrekking tot reeds plaatsgevonden datalekken alsnog geïnformeerd moet worden aan de betrokkenen (en eventueel derden) als gevolg van (technische) ontwikkelingen.

16. Handelswijze Autoriteit persoonsgegevens na melding en handhaving

Dit hoofdstuk bespreekt wat de AP doet in het geval de school een datalek meldt aan de AP. Ook gaat dit hoofdstuk in op de handhaving bij overtreding van de meldplicht door de school.

16.1. Administratieve afhandeling

Na het melden van een datalek ontvangt de school per omgaande een ontvangstbevestiging. Als de melding de AP aanleiding geeft tot nadere actie, dan zal de AP daarover contact met de school opnemen. In eerste instantie zal het daarbij gaan om verificatie dat de gedane melding daadwerkelijk van de school afkomstig is, en om eventuele inhoudelijke vragen over de melding die op dat moment (reeds) zouden bestaan.

16.2. Inhoudelijke afhandeling

Het is de verantwoordelijkheid van de school om de oorzaak van het datalek op te sporen, en om maatregelen te treffen om herhaling te voorkomen. Het is ook aan de school om te bepalen of zij de betrokkenen informeert en op welke manier zij dit doet. Dit handboek dient om de school in die besluitvorming te ondersteunen. De AP biedt, als toezichthouder, geen ondersteuning bij de afhandeling van een concreet datalek.

De ontvangen datalekmeldingen stellen de AP in staat om erop toe te zien dat betrokkenen adequaat worden geïnformeerd over datalekken die hen persoonlijke raken, of waarvan zij last kunnen ondervinden. Als de school het datalek niet heeft gemeld aan de betrokkene kan de AP, indien deze van oordeel is dat het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene, verlangen dat de school alsnog een kennisgeving doet (artikel 58 lid 2e AVG). Het niet nakomen van dit bevel door de AP levert een overtreding op die is onderworpen aan een administratieve geldboete. Zie voor de hoogte van deze boete paragraaf 16.4.

Ook kan de AP op basis van de ontvangen datalekmeldingen actie ondernemen om de adequate beveiliging van persoonsgegevens (binnen de school) meer in de breedte te bevorderen. Als uit de ontvangen datalekmeldingen blijkt dat de beveiliging van persoonsgegevens mogelijk niet op orde is, dan kan dat voor de AP aanleiding vormen voor nader onderzoek naar de naleving van de beveiligingsverplichtingen uit de AVG binnen de school.

16.3. Register van ontvangen datalekmeldingen

De AP houdt een register bij van de ontvangen datalekmeldingen. Dit register is niet openbaar. Het belang bij het vertrouwelijk blijven van gegevens over de beveiliging van de gegevensverwerking of over gelekte persoonsgegevens staat daaraan in de weg. Wel kan de AP op basis van de gedane meldingen in jaarverslagen of andere publicaties op geanonimiseerd en geabstraheerd niveau aandacht besteden aan datalekken bij de school.

16.4. Handhaving

De AP heeft een onderzoeksbevoegdheden, corrigerende bevoegdheden en adviserende bevoegdheden (artikel 58 AVG). Daarnaast kan de AP een administratieve geldboete opleggen (artikel 83 AVG). De AVG kent twee categorieën geldboeten. Een relatief lage geldboete van maximaal € 10.000.000,00 of 2% van de jaaromzet wanneer de AP constateert dat administratieve bepalingen zijn overtreden en een hoge geldboete van maximaal € 20.000.000,00 of 4% van de jaaromzet voor meer fundamentele overtredingen of het niet opvolgen van bevelen van de AP.

Onderzoek door de AP

De AP kan en mag:

- van de school (en haar verwerkers) gelasten om informatie te verstrekken die de AP nodig heeft om haar taken uit te kunnen voeren. De school is verplicht hieraan mee te werken;
- onderzoek verrichten in de vorm van gegevensbeschermingscontroles (audit);
- een toetsing verrichten van eventueel conform artikel 42 lid 7 AVG afgegeven certificeringen;
- de school (of verwerker) in kennis stellen van een beweerde inbreuk op de AVG;
- toegang vorderen tot persoonsgegevens en andere noodzakelijke informatie;
- toegang vorderen tot ruimten in de school en hulpmiddelen waarmee persoonsgegevens worden verwerkt (bijvoorbeeld relevante software).

Corrigerende maatregelen door de AP

Naast de onderzoeksbevoegdheden mag de AP ook corrigerende maatregelen nemen, te weten:

- waarschuwen en berispen;
- de school gelasten tot uitvoeren van een specifiek recht van betrokkene (bijvoorbeeld het wissen van gegevens);
- de school gelasten om binnen een bepaalde termijn verwerkingen in overeenstemming te brengen met de AVG;
- de school gelasten om een inbreuk aan de betrokkene mee te delen;
- het opleggen van een tijdelijk of definitief verwerkingsbeperking of -verbod;
- de school gelasten om persoonsgegevens te rectificeren, wissen of verwerkingen te beperking en dit mee te delen aan betrokkene;
- een certificering in te (laten) trekken.

Adviezen door de AP

De AP heeft de bevoegdheid om adviezen te verstrekken (zoals in voorkomend geval het verplichte advies voorafgaand aan bepaalde gegevensbeschermingseffectbeoordelingen of bijvoorbeeld advies aan sectororganisaties over toepassing van de AVG) en om certificeringen en gedagscodes goed te keuren. Adviezen die op basis van deze bevoegdheid worden gegeven kunnen worden aangemerkt als een besluit in de zin van de Algemene wet bestuursrecht (Awb). Hiertegen staat bezwaar en beroep open.

Het opleggen van een geldboete door de AP

De AP kan bij overtreding van de verplichtingen uit de AVG een geldboete opleggen. De AP houdt bij het bepalen van de hoogte van de boete rekening met alle omstandigheden van het geval en dient gemotiveerd aan te geven hoe men aan het betreffende bedrag komt (artikel 83 lid 2 AVG). Hierbij betrekt de AP onder meer de aard, ernst en duur van de inbreuk en het aantal getroffen betrokkenen alsmede de door hen geleden schade.

Daarnaast zijn er boeteverhogende omstandigheden (bijv. recidive of tegenwerking onderzoek AP) en boeteverlagende omstandigheden (bijv. vergaande medewerking met AP of eigener beweging schadeloosstellen gedupeerden) die de AP bij de vaststelling van de boete kan meewegen.

Type schending	Maximale boetebedrag
I. schending van een verplichting van procedurele aard (artikel 84 lid 4 AVG) Toelichting: categorie I. ziet specifiek op schendingen van verplichtingen overeenkomstig de artikelen 8, 11, 25 t/m 39, 41 lid 4, 42 en 43 van de AVG.	€ 10.000.000,00 of 2% van de jaaromzet
II. schending van een meer principiële verplichting of die de privacy van betrokkene directer raakt (artikel 83 lid 5 AVG) en het niet opvolgen van een bevel van de AP (artikel 83 lid 6 AVG) Toelichting: categorie II. ziet specifiek op schendingen van verplichtingen overeenkomstig de artikelen 5, 6, 7, 9, 12 t/m 22, 44 t/m 49, krachtens hoofdstuk IX door Nederland vastgesteld recht en artikel 58 lid 1 en 2 van de AVG.	€ 20.000.000,00 of 4% van de jaaromzet

17. Evaluatie handboek

De FG zal minimaal eenmaal per jaar, of zoveel eerder als noodzakelijk mocht blijken, een vergadering beleggen met de vaste leden van het IRT om dit handboek en bijbehorende bijlagen te evalueren en te bezien of de uitgangspunten van dit handboek aanpassing behoeven in het kader van ontwikkelingen/wijzigingen in de wetgeving, rechtspraak of binnen de (organisatie van de) school zelf.

18. Bijlagen

1.1.1. Bijlage VII-B Protocol Beveiligingsincidenten

1.1.2. Bijlage VII-C Formulier gegevens datalek

1.1.3. Bijlage VII-D Meldformulier

1.1.4. Bijlage VII-E Registratie datalekken (door verwerkingsverantwoordelijke)

Bijlage XII-B Protocol beveiligingsincidenten

Artikel 1. Doel van dit protocol

Het doel van dit protocol is tweeledig. Enerzijds dient het een personeelslid bewust te maken wat een inbreuk op de beveiliging is of kan zijn en anderzijds dient het personeelslid te informeren op welke wijze hij een mogelijk beveiligingsincident (dat mogelijk tevens een datalek blijkt te zijn) dient te signaleren.

Artikel 2. Begripsbepalingen

1. personeel(slid): het personeel als bedoeld in hoofdstuk 3 van het Handboek Datalekken;
2. beveiligingsincident: is een inbreuk op de beveiliging die mogelijk leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
3. datalek: is een inbreuk op de beveiliging die wel leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
4. persoonsgegevens: de gegevens als bedoeld in artikel 1 van het Privacyreglement;
5. FG: de functionaris gegevensbescherming.

Artikel 3. Meldplicht datalekken

Sinds 1 januari 2016 dient een verwerkingsverantwoordelijke (in dit geval de school) een zogenaamd datalek onverwijld te melden aan de Autoriteit Persoonsgegevens (AP) en mogelijk ook aan de betrokkene(n) (in dit geval veelal het personeel of de (ouders en/of verzorgers van de) leerlingen. Van een datalek die moet worden gemeld is sprake indien er persoonsgegevens verloren gaan of onrechtmatig worden verwerkt en het waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

In het kader van deze wettelijke plicht heeft de school een Handboek Datalekken opgesteld en geïmplementeerd. Onderdeel daarvan is ook dit protocol. Als het schoolbestuur namelijk niet op de hoogte is van een mogelijk beveiligingsincident zal het Handboek Datalekken niet in werking (kunnen) treden. Het schoolbestuur is dan ook afhankelijk van de input die zij in dit verband krijgt van onder andere het personeel.

Artikel 4. Meldingsplicht personeel

Een personeelslid is verplicht een (mogelijk) beveiligingsincident dat hij/zij ontdekt direct per e-mail of telefonisch te melden aan de FG ongeacht het tijdstip van de dag. Deze melding zal zo concreet mogelijk zijn. Het personeelslid neemt daarbij de inhoud van dit protocol in acht.

In dit verband geldt dat een personeelslid bij twijfel of er sprake is van een mogelijk beveiligingsincident toch meldt aan de FG.

Artikel 5. Persoonsgegevens

Wat zijn persoonsgegevens? Dit zijn niet alleen gegevens zoals naam, adres, woonplaats of BSNnummer. Deze gegevens worden aangeduid als direct identificerende gegevens. Daarnaast zijn er ook indirect identificerende gegevens. Dit zijn gegevens die iets zeggen over een natuurlijk persoon omdat zij gekoppeld kunnen worden aan een direct persoonsgegeven. Indien kan worden

achterhaald om welke natuurlijke persoon het gaat, is er sprake van een persoonsgegeven. Het kan dus onder andere gaan om:

- naam;
- adres;
- telefoonnummer;
- e-mailadres;
- salarisgegevens;
- gegevens met betrekking tot ziekte;
- beoordelingsgesprekken;
- studieadviezen;
- gegevens met betrekking tot gezondheid;
- dyslexie;
- betalingsachterstanden;
- gegevens over gezinssituatie;
- geloof;
- ras;
- studieresultaten;
- etc.

Artikel 6. Soorten beveiligingsincidenten

Er zijn verschillende soorten beveiligingsincidenten. Sommige beveiligingsincidenten zijn het gevolg van menselijke fouten, onoplettendheid of technisch falen. Deze beveiligingsincidenten worden niet bewust gecreëerd. Veel beveiligingsincidenten worden echter bewust gecreëerd.

Niet bewuste incidenten

Bij niet bewuste beveiligingsincidenten gaat het om incidenten die niet met opzet worden gecreëerd. Te denken valt aan:

- het laten liggen door van een laptop, tablet, smartphone of papieren dossier in de trein;
- het verliezen van een USB-stick, mobiele telefoon of bijvoorbeeld laptop;
- door haperende beveiliging (technische storing) zijn mogelijk persoonsgegevens van leerlingen ingezien door onbevoegden;
- de ruimte op school met daarin de fysieke leerlingdossiers heeft per ongeluk niet op slot gezeten voor een bepaalde periode;
- een docent heeft per ongeluk onbeheerd zijn laptop in de klas laten staan met daarop een memo-sticker met zijn inlognaam en wachtwoord;
- het verzenden door een medewerker van e-mail met vertrouwelijke gegevens aan de verkeerde ontvanger;
- het verzenden van een e-mail aan meerdere ontvangers die elkaars emailadressen niet kennen (zonder gebruik te maken van de bcc-optie);
- het crashen van een harde schijf met daarop persoonsgegevens;
- brand in een serverruimte of archiefruimte van de school;
- één van de hier voor genoemde situaties zich voordoet bij een verwerker van de school (bijvoorbeeld: de uitgever van digitale leermiddelen en Magister) voor zover het persoonsgegevens betreft van personeel of (ouder(s) en/of verzorger(s) van) leerlingen van de school.

Bewuste incidenten

Bij bewuste beveiligingsincidenten gaat het om incidenten die met opzet worden gecreëerd. Te denken valt aan:

- fysieke diefstal van een laptop, tablet, smartphone of (onderdelen van een) papieren dossier;
- het kopiëren, meenemen of bijvoorbeeld vernietigen van persoonsgegevens door personeel bijvoorbeeld uit onvrede over ontslag of studieadvies, als vriendendienst of als gevolg van chantage;
- phishing: het uitbuiten van menselijke kwetsbaarheden door hen onder valse voorwendselen persoonsgegevens te ontfutselen via mail of internet;
- hack: het uitbuiten van kwetsbaarheden in informatiesystemen en webservers;
- één van de hier voor genoemde situaties zich voordoet bij een bewerker van de school (bijvoorbeeld: de uitgever van digitale leermiddelen en Magister) voor zover het persoonsgegevens betreft van personeel of (ouder(s) en/of verzorger(s) van) leerlingen van de school.

Indien zich een dergelijk onbewust of bewust gecreëerd incident – of soortgelijkend incident – voordoet, is er sprake van een beveiligingsincident en dient het personeelslid dit te melden aan de FG.

Bijlage XII-C Formulier gegevens datalek

Deze bijlage bevat een aantal onderdelen van de gegevens die de School moet opgeven als zij een datalek meldt aan de AP. Bij het formulier zijn de vragen uit bijlage 1 bij de Europese Verordening 611/2013 als uitgangspunt gehanteerd. Het IRT gebruikt deze vragen om de benodigde informatie zo volledig en juist mogelijk te krijgen met betrekking tot het mogelijke datalek.

Gegevens over het datalek

1) Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
2) Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul aantallen in.)
    a) Minimaal: [vul aan]
    b) Maximaal: [vul aan]
3) Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
4) Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)
    a) Op [datum]
    b) Tussen [begindatum periode] en [einddatum periode]
    c) Nog niet bekend
5) Wat is de aard van de inbreuk? (De School kan meerdere mogelijkheden aankruisen.)
    a) Lezen (vertrouwelijkheid)
    b) Kopiëren
    c) Veranderen (integriteit)
    d) Verwijderen of vernietigen (beschikbaarheid)
    e) Diefstal
    f) Nog niet bekend
6) Om welk type persoonsgegevens gaat het? (De School kan meerdere mogelijkheden aankruisen.)
    a) Naam-, adres- en woonplaatsgegevens
    b) Telefoonnummers
    c) E-mailadressen of andere adressen voor elektronische communicatie
    d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
    e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
    f) Burgerservicenummer (BSN) of sofinummer
    g) Paspoortkopieën of kopieën van andere legitimatiebewijzen
    h) Geslacht, geboortedatum en/of leeftijd
    i) Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)

j) Overige gegevens, namelijk [vul aan]

7) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (De School kan meerdere mogelijkheden aankruisen.) a) Stigmatisering of uitsluiting

b) Schade aan de gezondheid

c) Blootstelling aan (identiteits)fraude

d) Blootstelling aan spam of phishing

e) Anders, namelijk [vul aan]

Vervolgacties naar aanleiding van het datalek

8) Welke technische en organisatorische maatregelen heeft de School getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Technische beschermingsmaatregelen

9) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)

a) Ja

b) Nee

c) Deels, namelijk: [vul aan]

10) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als de School bij vraag 24 gekozen heeft voor optie a of optie c. Als de School gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Bijlage XII-D Meldformulier

Gegevens over het datalek

1) Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

2) Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul aantallen in.)

a) Minimaal: [vul aan]

b) Maximaal: [vul aan]

3) Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

4) Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)

a) Op [datum]

b) Tussen [begindatum periode] en [einddatum periode]

c) Nog niet bekend

5) Wat is de aard van de inbreuk? (De School kan meerdere mogelijkheden aankruisen.)
   a) Lezen (vertrouwelijkheid)
   b) Kopiëren
   c) Veranderen (integriteit)Verwijderen of vernietigen (beschikbaarheid)
   d) Diefstal
   e) Nog niet bekend
6) Om welk type persoonsgegevens gaat het? (De School kan meerdere mogelijkheden aankruisen.)
   a) Naam-, adres- en woonplaatsgegevens
   b) Telefoonnummers
   c) E-mailadressen of andere adressen voor elektronische communicatie
   d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
   e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
   f) Burgerservicenummer (BSN) of sofinummer
   g) Paspoortkopieën of kopieën van andere legitimatiebewijzen
   h) Geslacht, geboortedatum en/of leeftijd
   i) Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
   j) Overige gegevens, namelijk [vul aan]
7) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (De School kan meerdere mogelijkheden aankruisen.) a) Stigmatisering of uitsluiting
   b) Schade aan de gezondheid
   c) Blootstelling aan (identiteits)fraude
   d) Blootstelling aan spam of phishing
   e) Anders, namelijk [vul aan]

Vervolgacties naar aanleiding van het datalek

8) Welke technische en organisatorische maatregelen heeft de School getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Technische beschermingsmaatregelen

9) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)
   a) Ja
   b) Nee

c) Deels, namelijk: [vul aan]

10) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als de School bij vraag 24 gekozen heeft voor optie a of optie c. Als de School gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Vervolgacties naar aanleiding van het datalek

11) Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Inlichten van de betrokkenen

12) Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (Kies een van de volgende opties.)

a) Ja

b) Nee

c) Nog niet bekend

13) Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord. Kies een van de volgende opties en vul waar nodig aan.)

a) Ik heb het datalek aan de betrokkenen gemeld op [datum]

b) Ik ga het datalek aan de betrokkenen melden op [datum]

c) Nog niet bekend

14) Wat is de inhoud van de melding aan de betrokkenen? (Letterlijke weergave, beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

15) Hoe veel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

16) Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

17) Waarom ziet u af van het melden van het datalek aan de betrokkenen? (Beantwoord deze vraag als u vraag 18 met nee hebt beantwoord. Kies een van de onderstaande opties en vul waar nodig aan.)

a) De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten.

b) Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: [vul aan]

c) Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: [vul aan]

d) Anders, namelijk: [vul aan]

Technische beschermingsmaatregelen

18) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)

a) Ja

b) Nee

c) Deels, namelijk: [vul aan]

19) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij vraag 24 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Internationale aspecten

20) Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)

a) Ja

b) Nee

c) Nog niet bekend

21) Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?

a) Ja, namelijk: [vul aan]

b) Nee

Vervolgmelding

22) Is naar uw mening deze melding compleet? (Kies een van de onderstaande opties.)

a) Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig

b) Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

Bijlage XII-E Registratie Datalekken [naam school]

Korte omschrijving van het lek:	
Wanneer vond het lek plaats?	
Wat is er met de gegevens gebeurd? (verloren gegaan/door een onbevoegde ingezien/ gekopieerd/gewijzigd)	

Van wie (welke groepen) zijn gegevens gelekt?	
Om hoeveel personen gaat het?	
Om welke persoonsgegevens gaat het?	
Wat zijn de (mogelijke) gevolgen van de inbreuk (bijvoorbeeld risico op identiteitsfraude of reputatieschade)	
Welke maatregelen zijn genomen naar aanleiding van het lek? (schadebeperking)	
Welke maatregelen zijn genomen om te zorgen dat het niet nog een keer kan gebeuren?	

Bijlage VIII Privacyverklaring

Ingangsdatum: 01-01-2019

Datum laatste wijziging: 01-01-2019

Stichting Christelijk Onderwijs Over- en Midden-Betuwe neemt privacy serieus. In deze privacyverklaring leggen wij uit welke persoonsgegevens wij verzamelen en gebruiken, met welk doel wij dit doen en hoe wij ervoor zorgen dat deze persoonsgegevens goed zijn beveiligd.

🕮 Privacybeleid

Stichting Christelijk Onderwijs Over- en Midden-Betuwe verwerkt, beheert en beveiligt persoonlijke gegevens als verwerkingsverantwoordelijke met de grootste zorgvuldigheid. Wij bieden onze leerlingen een veilige leeromgeving en onze medewerkers een veilige werkplek. We voldoen daarbij aan de eisen die de Algemene verordening gegevensbescherming (AVG) en nationale wetgeving aan

ons stelt. Hoe wij aan deze eisen voldoen hebben wij vastgelegd in ons Privacyreglement (https://www.sgomb.nl/privacyreglement).

Persoonsgegevens die wij verwerken

Stichting Christelijk Onderwijs Over- en Midden-Betuwe verwerkt persoonsgegevens van leerlingen, personeel, bezoekers en andere personen. Een deel van die persoonsgegevens ontvangen wij rechtstreeks van de betrokkenen. Bijvoorbeeld de NAW-gegevens via het inschrijvingsformulier voor leerlingen en bij het in dienst nemen van personeel. Een deel van de persoonsgegevens die wij verwerken verzamelen wij zelf, zoals voortgangsgegevens van leerlingen en gegevens over het functioneren van medewerkers. Verder ontvangen wij ook persoonsgegevens van derden.

Meer informatie over de persoonsgegevens die wij verwerken van leerlingen en personeel https://www.sgomb.nl/Privacyreglement.

Waarom wij persoonsgegevens gebruiken

Wij verzamelen en gebruiken persoonsgegevens hoofdzakelijk om onderwijs te organiseren. Dit betekent dat wij persoonsgegevens van leerlingen gebruiken om onderwijs te geven en leerlingen begeleiding te bieden. Persoonsgegevens van personeel gebruiken wij alleen met het oog op het uitvoeren van de arbeidsovereenkomst. Meer informatie https://www.sgomb.nl/Privacyreglement

Beveiligen en bewaren

De school neemt passende maatregelen om misbruik, verlies, onbevoegde toegang en andere ongewenste handelingen met persoonsgegevens tegen te gaan. Zo slaan wij persoonsgegevens op in systemen die beperkt toegankelijk zijn en maken wij gebruik van versleuteling. Deze maatregelen zijn opgenomen in ons veiligheidsbeleid. Meer informative https://www.sgomb.nl/Privacyreglement.

De verzamelde persoonsgegevens worden niet langer bewaard dan noodzakelijk is. Gegevens van leerlingen verwijderen wij twee jaar na uitschrijving. Voor personeel geldt hetzelfde, tenzij de school zich moet houden aan (een langere) bewaartermijn uit de wet. Meer informative https://www.sgomb.nl/Privacyreglement.

Deelt de school persoonsgegevens met derden?

Wij delen persoonsgegevens alleen met derden als dit nodig is voor de uitvoering van een overeenkomst of om te voldoen aan een wettelijke verplichting. Met organisaties die uw gegevens verwerken in opdracht van de school worden afspraken gemaakt om ervoor te zorgen dat uw gegevens ook daar goed zijn beveiligd. De school maakt ook gebruik van clouddiensten waarbij gegevens op een server in het buitenland worden opgeslagen. Dit doen wij alleen als sprake is van een adequaat niveau van gegevensbescherming. Meer informatie https://www.sgomb.nl/Privacyreglement.

Melding misstanden

Ook als u een melding doet van een misstand in onze organisatie, zullen uw gegevens worden verwerkt. U kunt daarom ook een melding doen bij de door onze school aangewezen functionaris doen. Deze functionaris kan door u in vertrouwen worden benaderd. Deze gegevens zullen zonder uw toestemming niet worden gedeeld met de schoolleiding. Voor meer informatie over de regeling verwijzen wij u naar de voor onze organisatie vastgestelde klokkenluidersregeling.

Welke rechten heb ik?

U heeft het recht om bezwaar te maken tegen de verwerking van uw gegevens, eerder gegeven toestemming in te trekken en u heeft het recht om uw gegevens in te zien, te corrigeren of te verwijderen. Ook kunt u in voorkomende gevallen aan de school vragen om de verwerking van uw persoonsgegevens te beperken of om uw gegevens aan uzelf of aan een derde partij over te dragen.

Wilt u gebruik maken van (een van) deze rechten of heeft u vragen over hoe wij omgaan met privacy en persoonsgegevens. Dan kunt u contact opnemen met de school Stichting Christelijk Onderwijs Over- en Midden-Betuwe via www.sgomb.nl of rechtstreeks met onze Functionaris voor de Gegevensbescherming (FG) .

Heeft u een klacht over de manier waarop wij persoonsgegevens verwerken? Neem ook dan contact op met onze FG via de hiervoor genoemde contactgegevens. Mocht u er samen met ons onverhoopt niet uitkomen, dan kunt u een klacht indienen bij de toezichthouder, de Autoriteit Persoonsgegevens via (https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-over-gebruikpersoonsgegevens).

✍ Aanpassen privacyverklaring

Wij behouden ons het recht voor deze privacyverklaring aan te passen. Op deze website plaatsen wij eventuele herziene versies. Als een herziene versie wordt geplaatst zorgen wij voor een duidelijke melding hiervan met informatie over de belangrijkste wijzigingen. Ook geven wij aan wanneer de verklaring voor het laatst is gewijzigd.

Toelichting

Volgens de AVG moeten persoonsgegevens niet alleen worden verwerkt op een rechtmatige en behoorlijke manier, maar ook op een wijze die transparant is (art. 5 lid1a AVG). Naast het informeren van de betrokkene voorafgaand aan de gegevensverwerking waarborgt de school deze transparantie door deze beknopte en toegankelijke privacyverklaring beschikbaar te maken voor betrokkene(n), door de verklaring te plaatsen op de website van de scholengroep.