STICHTING OPENBAAR VOORTGEZET ONDERWIJS PROGRESSO

PRIVACYREGLEMENT STICHTING PROGRESSO

Vastgesteld door het bevoegd gezag: 25 september 2018
Instemming Centrale Medezeggenschapsraad: 24 september 2018
Inwerkingtreding: 1 mei 2018

PRIVACY BIJ PROGRESSO

Wij bieden onze leerlingen en medewerkers een veilige leer- en werkplek. Een goede en zorgvuldige omgang met persoonsgegevens binnen de school is daarvoor een randvoorwaarde. Wij nemen de omgang met persoonsgegevens serieus en beogen een hoogwaardig veiligheidsniveau te bieden.

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

Met dit reglement beoogt Stichting Progresso ervoor zorg te dragen dat op de scholen van Stichting Progresso de verwerking van persoonsgegevens plaatsvindt conform de AVG, de uitvoeringswet, sectorgedragscodes, sectorbeveiligingscodes en 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.

Stichting Progresso heeft de ambitie om het eigen compliance-niveau naar een hoger niveau te tillen en zich als een volwassen organisatie te profileren op het gebied van privacy en informatiebeveiliging. Voldoen aan de geldende wet- en regelgeving is voor ons het speerpunt. Wij zullen ons beleid en de maatregelen ook hierop richten.

Het College van Bestuur zal in samenspraak met de Functionaris Gegevensbescherming en de Privacy Officer 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 zijn de begripsbepalingen en definities van artikel 4 van de AVG van overeenkomstige toepassing, voor zover deze niet verder worden gespecificeerd in artikel 1 van dit reglement. Verder wordt verstaan onder:

a) AVG: 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;
b) Autoriteit Persoonsgegevens: toezichthoudende autoriteit, als bedoeld in artikel 51 van de AVG;
c) Betrokkene: degene op wie een persoonsgegeven betrekking heeft (een sollicitant, een medewerker werkzaam/werkzaam geweest bij Stichting Progresso, een leerling ingeschreven/ingeschreven geweest aan een school behorende tot Stichting Progresso of een ouder/verzorger van wie gegevens in de persoonsregistratie zijn opgenomen, alle overige personen werkzaam bij of ten dienste van de Stichting Progresso, waaronder de leden van het toezichthoudend orgaan, leveranciers en dienstverleners, en tenslotte de bezoekers van één van de schoolgebouwen van de Stichting Progresso);
d) PIA: een gegevensbeschermingseffectbeoordeling als genoemd in artikel 35 van de AVG; een beoordeling van het effect van de beoogde verwerking op de bescherming van persoonsgegevens;
e) Groep: een economische eenheid waarin rechtspersonen organisatorisch verbonden zijn (artikel 2:24 BW);
f) Leerling: persoon die onderwijs volgt, zal volgen of heeft gevolgd op een school van Stichting Progresso;
g) Leerling- of personeelsnummer: eenduidig nummer dat wordt gebruikt ten behoeve van efficiënte verwerking van persoonsgegevens;
h) Personeel: de bij Stichting Progresso werkzame directeur, (adjunct-)directeur of leraar, en overige medewerkers 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 24e1, vierde lid van de Wvo respectievelijk artikel 28i vierde lid van de Wec, voor zover die leden mede zijn aangesteld op een akte en de eerdergenoemde medewerker die zonder aanstelling is tewerkgesteld bij of ingeleend door Stichting Progresso;
i) School: een school als bedoeld in artikel 1 van de Wvo en de Wec die in stand wordt gehouden door Stichting Progresso;
j) 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;
k) Stichting: Stichting Openbaar Voortgezet Onderwijs Progresso;
l) Toezichthoudend orgaan: de Raad van Toezicht;
m) 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;
n) Verwerkingsverantwoordelijke: Stichting Progresso;
o) Wec: Wet op de expertisecentra;
p) Wvo: Wet op het voortgezet onderwijs.

ARTIKEL 2. VERANTWOORDELIJKHEDEN

1. Stichting Progresso 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 resp. het 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. De Stichting Progresso laat zich bij bovengenoemde taken adviseren door de functionaris gegevensbescherming.

ARTIKEL 3. DE FUNCTIONARIS GEGEVENSBESCHERMING

1. De Functionaris Gegevensbescherming vervult zijn taken en verplichtingen onafhankelijk van het bestuur.
2. De Functionaris Gegevensbescherming houdt intern toezicht op de naleving van de wet- en regelgeving, de in de onderwijssector vastgestelde gedragscodes, het beleid van Stichting Progresso of de verwerker met betrekking tot de bescherming van persoonsgegevens.
3. De Functionaris Gegevensbescherming adviseert over verwerkingsprocessen en ziet toe op de uitvoering en evaluatie ervan.
4. De Functionaris Gegevensbescherming 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.
5. De Functionaris Gegevensbescherming werkt samen met de toezichthoudende autoriteit (Autoriteit Persoonsgegevens).
6. Betrokkenen kunnen met de Functionaris Gegevensbescherming 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 AVG.
7. De Functionaris Gegevensbescherming brengt jaarlijks verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden en bevindingen.
8. De controlebevoegdheden van de Functionaris Gegevensbescherming zijn neergelegd in een interne regeling en omvatten:
   a) de bevoegdheid om ruimtes te betreden;
   b) de bevoegdheid om inlichtingen en inzage te vragen en om zaken te onderzoeken;
   c) de faciliteiten die aan de Functionaris Gegevensbescherming ter beschikking worden gesteld om zijn bevoegdheden goed te kunnen uitoefenen.
9. De Functionaris Gegevensbescherming is met betrekking tot zijn taken tot geheimhouding en vertrouwelijkheid gehouden.

ARTIKEL 4. INFORMATIE EN TOEGANG TOT PERSOONSGEGEVENS

1. Indien de gegevens van de betrokkene zelf worden verkregen, informeert Stichting Progresso betrokkene bij de verkrijging van de persoonsgegevens over:
   a) de volledige naam en de contactgegevens van Stichting Progresso 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 1 sub f AVG), het gerechtvaardigd belang van Stichting Progresso;
   d) de ontvangers of categorieën van ontvangers;
   e) in voorkomend geval, dat Stichting Progresso 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, 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.
2. Indien de gegevens niet van betrokkene afkomstig zijn verstrekt Stichting Progresso aan de betrokkene de informatie als genoemd in vorig lid 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.
3. Stichting Progresso 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. 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 een 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.

ARTIKEL 5. CATEGORIEËN VAN BETROKKENEN, DOELEINDEN EN PERSOONSGEGEVENS

ARTIKEL 5.1. LEERLINGEN

1. De verwerking van persoonsgegevens van leerlingen heeft ten doel:
   a) de toelating en inschrijving van de leerling bij de school (artikel 6 lid 1 sub e AVG;
   b) de organisatie of het geven van onderwijs, (individuele) schoolbegeleiding van leerlingen, het opstellen van een onderwijskundig rapport en het geven van studieadviezen (artikel 6 lid 1 sub c AVG);
   c) bij uitschrijving van een leerplichtige leerling het informeren van de vervolgschool over het gevolgde onderwijs en de behaalde studieresultaten (artikel 6 lid 1 sub c 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 1 sub c AVG);
   e) het uitvoeren van de op Stichting Progresso 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 Medezeggenschap scholen (WMS), de Leerplichtwet en daarop gebaseerde regelgeving (artikel 6 lid 1 sub c en e AVG);
   f) het verstrekken of ter beschikking stellen van leermiddelen (artikel 6 lid 1 sub c AVG);
   g) het geven van onderwijs met behulp van digitale leermiddelen en diensten van de informatiemaatschappij (artikel 6 lid 1 sub a AVG);
   h) het verstrekken van inloggegevens voor het schoolnetwerk en digitale leermiddelen en – diensten (artikel 6 lid 1 sub b AVG);
   i) het berekenen en vaststellen van ouderbijdragen (artikel 6 lid 1 sub b AVG);
   j) het behandelen van geschillen aanhangig gemaakt bij klachten- en geschillencommissies (artikel 6 lid 1 sub c AVG);
   k) het laten uitvoeren van een accountantscontrole (artikel 6 lid 1 sub c AVG);
   l) medewerking verlenen aan een aanvraag van ouders, respectievelijk leerlingen, voor leerlingenvervoer (artikel 6 lid 1 sub c 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 1 sub a AVG);
   n) het opstellen en vormgeven van een (digitaal) smoelenboek met de foto's van leerlingen (artikel 6 lid 1 sub a AVG);
   o) beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Stichting Progresso, waaronder in ieder geval het verstrekken van een leerlingpas (artikel 6 lid 1 sub f AVG);
   p) het uitvoering geven aan de wettelijke verplichting gegevens te verstrekken aan het Ministerie van Onderwijs, Cultuur 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 1 sub c AVG);
   q) het voldoen aan een verzoek van een bestuursorgaan dat is belast met de uitvoering van een publiekrechtelijke taak (artikel 6 lid 1 sub e AVG);
   r) het aanbieden van diensten door de schoolfotograaf (artikel 6 lid 1 sub a AVG).

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;
   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 cameraopnamen 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.

ARTIKEL 5.2. PERSONEEL

1. De verwerking van gegevens van personeel heeft ten doel:
   a) het aangaan van een arbeidsovereenkomst (artikel 6 lid 1 sub b AVG);
   b) het vaststellen van het salaris en overige arbeidsvoorwaarden (artikel 6 lid 1 sub b AVG);
   c) het (laten) uitbetalen van het salaris, de afdracht van belastingen en premies (artikelen 6 lid 1 sub b en c AVG);
   d) de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde (artikel 6 lid 1 sub b AVG);
   e) het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen (artikel 6 lid 1 sub b AVG);
   f) het verlenen van ontslag (artikel 6 lid 1 sub b 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 1 sub b AVG);
h) het geven van leiding en het begeleiden van betrokkene (artikel 6 lid 1 sub b AVG);
i) het verstrekken van de bedrijfsmedische zorg voor betrokkene en het kunnen nakomen van re-integratieverplichtingen bij verzuim (artikel 6 lid 1 sub c AVG);
j) het toegang verlenen tot het schoolnetwerk (artikel 6 lid 1 sub b AVG);
k) het regelen van en de controle van aanspraken op uitkeringen in verband met de beëindiging van het dienstverband (artikel 6 lid 1 sub b AVG);
l) de verkiezing van de leden van een bij wet of intern ingericht medezeggenschapsorgaan (artikel 6 lid 1 sub a en c AVG);
m) het behandelen van geschillen (artikel 6 lid 1 sub b AVG);
n) de behandeling van personeelszaken, anders dan genoemd onder a. t/m m. (artikel 6 lid 1 sub b AVG);
o) de organisatie of het geven van onderwijs (artikel 6 lid 1 sub b AVG);
p) het laten uitvoeren van een accountantscontrole en het laten vaststellen van aanspraken op bekostiging (artikel 6 lid 1 sub c AVG);
q) beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Stichting Progresso (artikel 6 lid 1 sub f AVG);

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.

ARTIKEL 5.3. SOLLICITANTEN

1. Stichting Progresso heeft een sollicitatiecode waarin de procedures van de organisatie inzake werving en selectie zijn opgenomen alsook de wijze van omgang met persoonsgegevens.
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 1 sub a en b AVG);
   b) de beoordeling van de geschiktheid van betrokkene voor een functie die in de nabije toekomst vacant kan komen (artikelen 6 lid 1 sub a en b AVG);
   c) de afhandeling van de door de sollicitant gemaakte onkosten (artikel 6 lid 1 sub a AVG);
   d) beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Stichting Progresso (artikel 6 lid 1 sub f AVG);
   e) de uitvoering of toepassing van wetgeving (artikel 6 lid 1 sub c AVG).

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.

ARTIKEL 5.4. OUD-MEDEWERKERS

1. De verwerking van gegevens van oud-medewerkers heeft ten doel:
   a) het onderhouden van contacten met oud-medewerkers (artikel 6 lid 1 sub a AVG);
   b) het verzenden van informatie aan oud-medewerkers (artikel 6 lid 1 sub a AVG);
   c) het verwerken van de aanmeldingen van oud-medewerkers voor mede voor hen georganiseerde activiteiten en bijeenkomsten (artikel 6 lid 1 sub a 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 1 sub a AVG);
   e) het doen uitvoeren van accountantscontrole (artikel 6 lid 1 sub c AVG).

2. 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) 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.

ARTIKEL 5.5. OUD-LEERLINGEN

1. De verwerking van gegevens van oud-leerlingen heeft ten doel:
   a) het onderhouden van contacten met de oud-leerlingen (artikel 6 lid 1 sub a AVG);
   b) het verzenden van informatie aan de oud-leerlingen (artikel 6 lid 1 sub a AVG);
   c) het verwerken van de aanmeldingen van oud-leerlingen voor mede voor hen georganiseerde activiteiten en bijeenkomsten (artikel 6 lid 1 sub a 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 1 sub a AVG);
   e) het doen uitvoeren van een accountantscontrole (artikel 6 lid 1 sub c AVG);
   f) het archiefbeheer, het behandelen van geschillen, het verrichten van wetenschappelijk, statistisch of historisch onderzoek (artikel 6 lid 1 sub a en f AVG).

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.

ARTIKEL 5.6. LEDEN VAN HET TOEZICHTHOUDEND ORGAAN

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 1 sub b AVG);
   b) het vastleggen en (laten) uitbetalen van de – door het toezichthoudend orgaan - vastgestelde beloning alsmede overige activiteiten van intern beheer (artikel 6 lid 1 sub b AVG);
   c) de aanmelding voor de aansprakelijkheidsverzekering voor toezichthouders (artikel 6 lid 1 sub b 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 1 sub c 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 1 sub b AVG);
   f) het onderhouden van contacten tussen Stichting Progresso en de medezeggenschapsraad met het toezichthoudend orgaan (artikel 6 lid 1 sub b AVG);
   g) het verzenden van (management)informatie aan het toezichthoudend orgaan (artikel 6 lid 1 sub b AVG);
   h) het laten uitvoeren van een accountantscontrole (artikel 6 lid 1 sub c AVG);
   i) beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Stichting Progresso (artikel 6 lid 1 sub f AVG).

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.

ARTIKEL 5.7. BEZOEKERS

1. De verwerking van gegevens van bezoekers van een van de gebouwen van de Stichting Progresso heeft ten doel:
   a) het interne beheer (artikel 6 lid 1 sub f AVG);
   b) beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Stichting Progresso (artikel 6 lid 1 sub f AVG).

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) camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;
   c) gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt.
3. Stichting Progresso informeert bezoekers van de websites (www.progresso.amsterdam, www.calandlyceum.nl, www.lumion.amsterdam) bij een bezoek aan de website over de doeleinden en gegevens die worden verwerkt bij een bezoek aan de website door middel van een privacystatement dat op de website van Stichting Progresso is geplaatst.

ARTIKEL 5.8. LEVERANCIERS/DIENSTVERLENERS

1. De verwerking van gegevens van leveranciers van Stichting Progresso heeft ten doel:
   a) het doen van bestellingen of de opdrachtverlening aan dienstverleners (artikel 6 lid 1 sub b AVG);
   b) het berekenen en vastleggen van inkomsten en uitgaven en het doen van betalingen (artikel 6 lid 1 sub b 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 1 sub b AVG);
   d) het onderhouden van contacten door de verwerkingsverantwoordelijke met de leveranciers (artikel 6 lid 1 sub b AVG);
   e) het behandelen van geschillen en het doen uitvoeren van een accountantscontrole (artikel 6 lid 1 sub c AVG);
   f) de uitvoering of de toepassing van een andere wet (artikel 6 lid 1 sub c AVG);
   g) beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Stichting Progresso (artikel 6 lid 1 sub f AVG).

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 camera-beelden zijn gemaakt.

ARTIKEL 6. RECHTEN VAN BETROKKENEN

ARTIKEL 6.1. PRIVACYVERKLARING

1. Stichting Progresso 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.

ARTIKEL 6.2. RECHT OP INFORMATIE

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.

ARTIKEL 6.3. RECHT OP RECTIFICATIE EN WISSING

1. Betrokkenen hebben het recht op rectificatie van onjuiste persoonsgegevens.
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 sub 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.

3. In het geval de te wissen gegevens openbaar zijn gemaakt en Stichting Progresso besluit de gegevens te wissen, neemt Stichting Progresso, 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.
4. De leden 1 en 2 zijn niet van toepassing als 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, ernstig in het gedrang dreigt te brengen of een onevenredige werkbelasting voorzien wordt .

ARTIKEL 6.4. RECHT OP BEPERKING VAN GEGEVENSVERWERKING

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 Stichting Progresso 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.

ARTIKEL 6.5. RECHT OP GEGEVENSOVERDRAAGBAARHEID

1. Betrokkene heeft recht de hem betreffende persoonsgegevens die hij zelf aan Stichting Progresso heeft verstrekt in een gestructureerde, gangbare en machine leesbare 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 1 sub a AVG) zijn verstrekt of op basis van een overeenkomst (artikel 6 lid 1 sub b AVG) en de verwerking via geautomatiseerde procedés wordt verricht.
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.
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.

ARTIKEL 6.6. INDIENING VAN EEN VERZOEK

1. Een verzoek als bedoeld in artikel 6 wordt gericht aan Stichting Progresso ter attentie van de Privacy Officer van de Stichting. Betrokkene kan zijn verzoek richten aan privacy@sovop.nl.
2. Aan een verzoek zijn geen kosten verbonden. Wanneer verzoeken van een betrokkene kennelijk ongegrond, buitensporig of een onredelijke werklast met zich meebrengen, met name vanwege hun repetitieve karakter kan Stichting Progresso echter een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verzoek gepaard gaat of weigeren gevolg geven aan het verzoek.
3. Stichting Progresso verstrekt de betrokkene binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven.
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.
5. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan de in vorig lid genoemde termijn indien nodig met nog eens twee maanden worden verlengd. Stichting Progresso 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. Indien Stichting Progresso 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.
7. Indien Stichting Progresso 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.

ARTIKEL 6.7. BEPERKINGEN

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

ARTIKEL 6.8. KLACHTRECHT

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 Stichting Progresso of de Autoriteit Persoonsgegevens benaderen met een verzoek tot bemiddeling.

ARTIKEL 7. BEVEILIGING

1. Stichting Progresso hanteert het voor de onderwijssector vastgestelde normenkader bij het vaststellen van passende technische en organisatorische maatregelen waartoe de verordening verplicht.
2. Stichting Progresso 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.

ARTIKEL 8. DE VERWERKER

1. De verwerkers zijn degenen die op basis van een overeenkomst voor of namens Stichting Progresso gegevens verwerken.
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.
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. De Functionaris Gegevensbescherming ziet erop toe dat de in het vorige lid bedoelde voorzieningen worden getroffen en in acht worden genomen.

ARTIKEL 9. INBREUK OP DE BEVEILIGING

1. Indien zich binnen de organisatie van Stichting Progresso of bij een door Stichting Progresso ingeschakelde verwerker een inbreuk op de beveiliging voordoet, waarbij een aanzienlijke kans bestaat op verlies of onrechtmatige verwerking van persoonsgegevens die door Stichting Progresso worden verwerkt, dan wel dit verlies of onrechtmatige verwerking zich daadwerkelijk voordoet, zal Stichting Progresso 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.
2. Stichting Progresso zal iedere inbreuk op de beveiliging als bedoeld in het eerste lid documenteren, ongeacht of deze wordt gemeld bij de Autoriteit Persoonsgegevens.
3. Indien de inbreuk een hoog risico voor de rechten en vrijheden van betrokkene inhoudt, stelt Stichting Progresso ook de betrokkene onverwijld in kennis van de inbreuk. Deze mededeling kan achterwege blijven indien de persoonsgegevens versleuteld zijn en niet toegankelijk zijn 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.

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 Stichting Progresso de procedures die zijn opgenomen in het handboek en protocol Datalekken.

ARTIKEL 10. KLACHTEN NALEVING VERORDENING

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 Functionaris Gegevensbescherming.
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.
3. (Ouders/verzorgers van) leerlingen en medewerkers kunnen zich tevens wenden tot de externe klachtencommissie waarbij Stichting Progresso is aangesloten: info@onderwijsgeschillen.nl.

ARTIKEL 11. INWERKINGTREDING, WIJZIGING EN CITEERTITEL

1. Dit reglement wordt aangehaald als ‘Privacyreglement’ en treedt in werking op de datum vermeld op het titelblad.
2. Het reglement is vastgesteld door Stichting Progresso en de medezeggenschapsraad en vervangt eventuele vorige versies.
3. Het reglement kan periodiek worden geëvalueerd met beide geledingen van de medezeggenschapsraad en kan indien dit wordt gewenst of nodig is om de AVG correct na te leven, worden gewijzigd, nadat instemming van de medezeggenschapsraad is verkregen.
4. Instemming wordt eveneens verleend voor wijzigingen die dit reglement of een van de bijlagen op basis van enig wettelijk of ministerieel voorschrift dient te ondergaan.
5. Het bevoegd gezag informeert de medezeggenschapsraad over dergelijke wijzigingen.

BIJLAGE I PROTOCOL VOOR HET GEBRUIK VAN E-MAIL, ICT EN SOCIALE MEDIA

Artikel 1 Werkingssfeer van deze regeling, begrippen

1. Deze regeling geeft de wijze aan waarop binnen Stichting Progresso 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.
2. Deze regeling geldt voor een ieder 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)'.
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.
4. Voor zover de gebruikers thuis of elders gebruik maken van de ICT (bijvoorbeeld het e-mailadres van de school of de schoolwebsite) zijn de bepalingen van deze regeling eveneens van toepassing.

Artikel 2 Toegang tot en gebruik van de ICT

1. De Stichting Progresso 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. Gebruikersidentificatie (gebruikersnaam) en authenticatie (wachtwoord) worden door de ICT-afdeling verstrekt en zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.
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

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.
2. Tijdens het gebruik van de ICT-apparatuur is het niet toegestaan etens- en drinkwaren te nuttigen.
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, uitzondering daarop is de koppeling van een laptop of device aan een smartboard of ander presentatiescherm.
4. De ICT-afdeling verleent alleen ondersteuning op apparatuur die door de ICT-afdeling is aangeschaft, aangesloten en geïnstalleerd.
5. Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) van de gebruikers is toegestaan 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;

6. Het gebruik van eigen computerapparatuur (bijvoorbeeld laptops of iPads) 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

1. Stichting Progresso behoudt zich het recht voor om de toegang tot bepaalde sites door middel van een filtersysteem te beperken.
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
   d) Aan alle externe e-mail wordt een disclaimer toegevoegd. Naar de tekst van deze disclaimer kan rechtstreeks worden gelinkt via: http://www.sovop.nl/disclaimer/
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. 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 Progresso – indien door haar niet langer aan deze voorwaarden kan worden voldaan - besluiten het gebruik van deze software door medewerkers te verbieden.

Artikel 5 Verantwoord gebruik van ICT

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 dit reglement.
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.

Artikel 6 Onverantwoord gebruik van ICT

1. Het is niet toegestaan om de ICT zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast.
2. Het is niet toegestaan zich toegang te verschaffen tot gegevens van andere gebruikers, tenzij met uitdrukkelijke toestemming van de betreffende gebruiker.
3. Het is niet toegestaan pogingen te ondernemen om het filtersysteem te omzeilen.
4. 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 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 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.
5. 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.
6. Het is ook anderszins niet toegestaan om door middel van de ICT in strijd met de wet of onethisch te handelen.
7. De schoolleiding kan de ICT-afdeling opdracht geven geconstateerde ongeoorloofde data van het computernetwerk te verwijderen.
8. Voor personeelsleden is het voor testdoeleinden toegestaan software lokaal te installeren die nodig is voor de werkzaamheden ten behoeve van school.
9. 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. Als de gebruiker eraan twijfelt of een bepaald gebruik van ICT wel verantwoord is, dan overlegt hij daarover met de ICT-afdeling.

Artikel 7 Algemene uitgangspunten van controle op gebruik

1. Het bevoegd gezag 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 AVG gehandeld worden.
2. Als een lid van de schoolleiding merkt of er op geattendeerd wordt dat het ICT-gedrag van een personeelslid niet binnen de kaders van dit reglement verloopt, wordt het personeelslid hierop door het bevoegd gezag gewezen en wordt een controle van zijn ICT-gebruik door bevoegde personen van de ICT-afdeling als mogelijkheid genoemd.
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 de schoolleider waaronder deze leerling ressorteert.
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.
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. In geval dat ten aanzien van een gebruiker, vanwege een concreet vermoeden van oneigenlijk gebruik, een gerichte controle is uitgevoerd, stelt het bevoegd gezag deze gebruiker daarvan zo spoedig mogelijk nadat de controle heeft plaatsgevonden van op de hoogte.
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.
8. Privémail/-gebruik (voorzien van het label ‘persoonlijk’) wordt zoveel mogelijk ontzien van controle.
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.
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 8 Doeleinden van controle

1. De controle op persoonsgegevens bij gebruik van ICT vindt slechts plaats met als doel:
   a. het tegengaan 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.
2. Onder ‘bewaking van de voortgang van de werkzaamheden’ 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.
3. Onder 'vastleggen van bewijs en/of archief' 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).
4. Onder 'systeem- en netwerkbeveiliging' wordt begrepen: controle op het email- en internetgebruik ter voorkoming van systeemaanvallen door onder andere virussen, trojans of andere schadelijke programma's.
5. Onder 'kosten- en capaciteitsbeheersing' als wordt begrepen: controle op het email- en internetgebruik ter inventarisering en/of beheersing van de kosten die gemoeid zijn met het gebruik van ICT.

Artikel 9 Specifieke uitgangspunten van controle op gebruik

1. In het kader van de controle op de gebruikers 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.
2. In het kader van de controle voor het doel als bedoeld in artikel 8 lid 1 sub b geldt dat slechts berichten worden verwerkt die rechtstreeks verband houden met uitvoering van de te verrichten taken door het personeelslid.
3. In het kader van de controle voor het doel als bedoeld in artikel 8 lid 1 sub b geldt dat slechts de emailverkeersgegevens en inhoud van de berichten wordt verwerkt.
4. In het kader van de controle voor het doel als bedoeld in artikel 8 lid 1 sub c geldt dat slechts zakelijke berichten worden verwerkt voor zover deze kunnen dienen als bewijs van zakelijke transacties en dossiervorming.
5. In het kader van de controle voor het doel als bedoeld in artikel 8 lid 1 sub c geldt dat slechts de e-mail en/of internetverkeersgegevens en inhoud van berichten wordt verwerkt.
6. In het kader van de controle voor het doel als bedoeld in artikel 8 lid 1 sub d 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.
7. In het kader van de controle voor het doel als bedoeld in artikel 8 lid 1 sub d geldt dat slechts de e-mailverkeersgegevens en inhoud (en bijlagen) van berichten met een verdachte inhoud worden gecontroleerd en de internetverkeersgegevens en inhoud van berichten met een verdachte inhoud worden gecontroleerd.

8. In het kader van de controle voor het doel als bedoeld in artikel 8 lid 1 sub e geldt dat de controle van het email- en internetverkeer beperkt blijft tot de verkeersgegevens.
9. In het kader van de controle voor het doel als bedoeld in artikel 8 lid 1 sub e geldt dat slechts de e-mailverkeersgegevens over tijd, hoeveelheid, omvang en dergelijke internet-verkeersgegevens over tijd en dergelijke worden verwerkt.

Artikel 10 Gebruik van social media

1. Onder social media wordt verstaan alle huidige en toekomstige online platformen waarbij de gebruikers de inhoud verzorgen.
2. Indien social media voor onderwijsdoeleinden worden gebruikt dient dit – met het oog op de bescherming van leerlinggegevens - plaats te vinden conform het Privacyreglement.
3. Voor het overig gebruik geldt dat dit grotendeels in eigen tijd dient plaats te vinden. Dat geldt ook voor het gebruik van social media door middel van smartphones of tablets.
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 Progresso en haar entiteiten.

Artikel 11 Richtlijnen voor het gebruik van social media

1. Voor zover de gebruiker op social media uitingen doet die in relatie staan tot Stichting Progresso geeft hij steeds duidelijk aan in welke relatie (bijvoorbeeld: personeelslid of leerling) hij staat tot de school.
2. De gebruiker plaatst op social media geen content met een onverantwoorde inhoud.
3. De gebruiker deelt op social media geen interne- of bedrijfsvertrouwelijke informatie over de school.
4. De gebruiker deelt geen persoonsgegevens van personeel of leerlingen waartoe hij uit hoofde van zijn functie toegang heeft.
5. De gebruiker laat zich op social media niet negatief of anderszins ongepast uit over Stichting Progresso en haar entiteiten, over collega's, over personeelsleden en/of over (mede-)leerlingen.
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.
7. De gebruiker plaatst op social media geen content namens Stichting Progresso, tenzij hij daarvoor toestemming heeft gekregen.
8. In zijn algemeenheid geldt dat de gebruiker op social media geen content zal plaatsen of zich anderszins zal gedragen op een wijze die Stichting Progresso of haar entiteiten schade kan toebrengen.

Artikel 12 Richtlijnen voor contact middels ICT

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.
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 de

schoolleiding. Het personeelslid mag het contact met de leerling uitsluitend onderhouden via het e-mailadres van de school.
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.
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, tablet of smartphone.
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.

Artikel 13 Clean desk beleid

Alle (flex-)werkplekken dienen na een werkdagen of bij afwezigheid gedurende een langere tijd opgeruimd te worden. Met name documenten die persoonsgegevens, gevoelige informatie, confidentiële informatie bevatten dienen uit het zicht en beveiligd opgeborgen te worden. Dit kan bewerkstelligd worden door een slot op een deur of een kast waartoe slechts een beperkt aantal personen toegang hebben. Drukwerk dat bij de printer wordt achtergelaten wordt in de papierbak gedaan.

Artikel 14 Vergrendeling ICT-apparatuur

Al het ICT-apparatuur dat (deels) zakelijk wordt gebruikt dient bij kortdurende afwezigheid vergrendeld te worden door middel van een unieke toegangscode, vingerafdruk of gezichtsherkenning. Deze vergrendeling dient over een complexiteit te beschikken waardoor het onmogelijk is voor een ander om toegang te verschaffen.

Artikel 15 Bring Your Own Device

Stichting Progresso faciliteert en ondersteunt de benodigde ICT-apparatuur voor uitvoering van de werkzaamheden. Indien een medewerker na de mogelijkheid tot of verstrekking van de nodige ICT-apparatuur wenst gebruik te maken van eigen apparatuur dan kan Stichting Progresso de ondersteuning van deze apparatuur weigeren. De medewerker is zelf verantwoordelijk voor een adequaat beveiligingsniveau en ondersteuning. De medewerker is aansprakelijk, indien benodigde apparatuur is verstrekt of de medewerker is gewezen op de mogelijkheid tot facilitering daarvan, voor (vervolg)schade die voortvloeit uit gebrekkig beveiligde apparatuur, beveiligingsincidenten, phishing, hacks, bugs of andere ongewenste informatietechnologische incidenten.

Artikel 16 Gebruik OneDrive

De opslag binnen de organisatie wordt verricht op OneDrive. Vanwege beveiligingsoverwegingen en ter voorkoming van datalekken dient er niets wat vertrouwelijk is of persoonsgegevens bevat, op de lokale schijf te worden opgeslagen. De medewerker is hier verantwoordelijk voor.

Artikel 17 Disciplinaire maatregelen bij leerlingen

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 18 Disciplinaire maatregelen bij personeelsleden

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

BIJLAGE II PROTOCOL GEBRUIK VAN CAMERA- EN VIDEOBEELDEN

Artikel 1 Doel van camera- en video-opnames

Het maken van (digitale)opnames heeft ten doel:

a. 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;
b. het begeleiden en coachen van medewerkers, in het bijzonder maar niet uitsluitend onderwijzend personeel in lessituaties.

Artikel 2 Begripsbepaling

1. camera's: het betreft camera's die bedoeld zijn voor algemeen toezicht;
2. camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten, glasvezelverbindingen en bevestigingen;
3. video-opnames: camera-opnames met als doel begeleiding en coaching van personeel;
4. beheer: zorg voor de continuïteit van het cameratoezicht;
5. functionaris gegevensbescherming: degene die is belast met het beheer van het camerasysteem;
6. beeldinformatie: de door het camerasysteem verkregen en geregistreerde filmbeelden.

Artikel 3 Plaats- en tijdbepaling cameratoezicht en video-opnames

1. Cameratoezicht vindt plaats op het schoolterrein van het Calandlyceum en Lumion. Binnen de school vindt cameratoezicht plaats in de werkkamer van de conciërges. De camera's zijn bij beweging van personen operationeel. Op het Lumion is het cameratoezicht doorlopend. Cameratoezicht vindt plaats door de hele school op algemeen toegankelijke plekken, met uitzondering van was, kleed- en toiletruimten.
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. 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

1. Het cameratoezicht en het maken van video-opnames geschiedt onder verantwoordelijkheid van het College van Bestuur.
2. Degene die belast is met het beheer van het camerasysteem zijn de conciërges van de gebouwen.
3. Bevoegd tot het bedienen van het camerasysteem en het bekijken van de beelden zijn conciërges en teamleiders.
4. Degenen die toegang hebben tot de camera en videobeelden zullen daarmee strikt vertrouwelijk omgaan. Zij zullen geheimhouding betrachten.
5. De beveiliging van het camerasysteem vindt plaats in overeenstemming met het Privacyreglement.

Artikel 5 Kenbaarheid

1. Het cameratoezicht wordt kenbaar gemaakt door middel van stickers op de plaatsen waar het cameratoezicht plaatsvindt en bij de ingang van het terrein.
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.
3. Alle personeelsleden en leerlingen worden geïnformeerd over dit protocol.
4. Voor betrokkenen (niet zijnde personeelsleden of leerlingen) ligt het protocol ter inzage bij de Privacy Officer, te bereiken op het mailadres; privacy@sovop.nl

Artikel 6 Doelbinding, zorgvuldigheid, bewaartermijnen en rechten van betrokkenen

1. De geregistreerde camera- en videobeelden worden uitsluitend gebruikt voor de doelstellingen zoals in dit protocol zijn verwoord.
2. Het gebruik van de camera- en videobeelden zal niet verder gaan dan strikt noodzakelijk is voor het doel waarvoor het toezicht is ingesteld.
3. De camerabeelden die gemaakt zijn met het oog op de veiligheid van de school worden na 2 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.
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.

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

Artikel 7 Heimelijk cameratoezicht

1. Heimelijk cameratoezicht kan worden ingezet indien er sprake is van een serieus en concreet vermoeden van diefstal, c.q. andere onrechtmatigheden en er niet in is geslaagd om met behulp van minder vergaande middelen – waaronder het reguliere cameratoezicht – tot uitkomsten te komen.
2. Het heimelijk cameratoezicht wordt in duur en omvang zo beperkt mogelijk gehouden.
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.

Artikel 8 Bewaartermijnen videobeelden

1. De videobeelden van de beveiligingscamera's worden voor 14 dagen bewaard. Daarna worden de videobeelden automatisch verwijderd.
2. Het eerste lid vindt geen toepassing indien er incidenten zijn opgenomen door de beveiligingscamera's. De beelden van de camera('s) worden dan aangehouden tot er duidelijkheid bestaat over de relevante beelden die kunnen dienen ter bewijsvergaring, opsporing door bevoegde diensten of uitvoering van interne disciplinaire procedures.
3. De videobeelden die bij toepassing van het tweede lid niet worden gebruikt worden zo snel als mogelijk verwijderd, doch op het moment dat duidelijk is dat er geen enkel belang bestaat bij bewaring van deze beelden.

BIJLAGE III HANDBOEK DATALEKKEN

Sinds 1 januari 2016 is een verwerkingsverantwoordelijke (in dit verband: de school) verplicht om een datalek te melden aan de Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens en/of de betrokkene.

Definities

De definities uit artikel 1 van het Privacyreglement zijn van overeenkomstige toepassing.

Onder het Incident Response Team (IRT) wordt verstaan; het team van professionals die binnen de lijnwerkzaamheden een belangrijke rol vervullen in de bescherming van persoonsgegevens, het waarborgen van privacy en het beveiligingsniveau binnen de organisatie en als zodanig in het IRT verantwoordelijk zijn voor afhandeling van beveiligingsincidenten en datalekken.

Signaleren van een beveiligingsincident

Medewerkers worden onder andere door middel van het protocol Beveiligingsincidenten (bijlage IV) 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 Privacy Officer (privacy@sovop.nl) ongeacht het tijdstip van de dag.

De Privacy Officer meldt vervolgens op zijn beurt per omgaande het beveiligingsincident telefonisch aan het bestuur c.q. de bestuurssecretaris en de Functionaris Gegevensbescherming en bevestigt dit 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 Privacy Officer (privacy@sovop.nl). Door middel van de melding wordt de procedure als verwoord in dit handboek daadwerkelijk gestart.

Incident Response Team

Nadat de melding is binnengekomen en een inschatting is gemaakt van de gevolgen komt het IRT op de kortst mogelijke termijn bijeen om het beveiligingsincident in kaart te brengen. De Privacy Officer doet zo snel als mogelijk verslag bij het bestuur en de Functionaris Gegevensbescherming.

Het IRT bestaat uit de volgende vaste leden:

1) de Privacy Officer
2) de afdeling ICT
3) de Bestuurssecretaris

Zo nodig wordt het IRT – na een afweging daartoe - aangevuld met:

4) de Bestuurder
5) de Functionaris Gegevensbescherming
6) de (school)directeur
7) de teamleider van een betrokken afdeling

De Privacy Officer is tevens de voorzitter van het IRT en heeft de plicht er voor zorg te dragen dat de leden beschikbaar zijn, worden opgeroepen en op de hoogte zijn van hun (mogelijke) rol binnen het IRT. Het IRT opereert vanuit het Bestuursbureau van Stichting Progresso.

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 heeft ieder lid een adviserende stem. Besluiten worden genomen door de Bestuurssecretaris en 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.

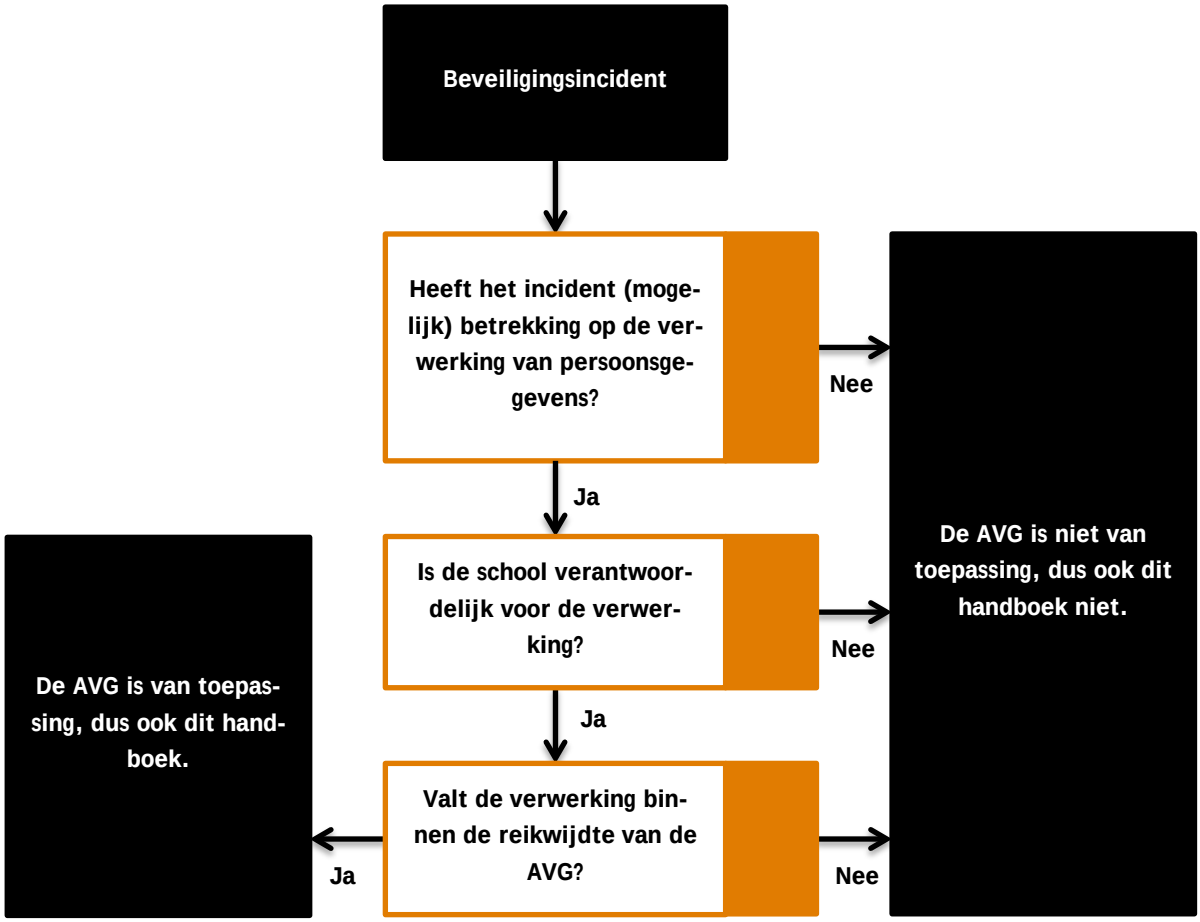
Bij het verzamelen van de benodigde informatie hebben de leden van het IRT en de FG, althans door hun aangewezen derden - toegang tot alle plekken en ruimtes binnen de school, zijn zij gerechtigd tot inzage in alle informatie, bestanden en/of data die hen geraden voorkomt en kunnen zij met iedereen spreken. 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.

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.

Eerste beoordeling: is de AVG van toepassing?

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



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[1] of hashing[2] 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 redelijkerwijs tot een persoon te herleiden is, kan door technische ontwikkelingen alsnog een persoonsgegeven worden als gevolg van de toegenomen mogelijkheden tot herleiding.

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 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.

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).

Tweede beoordeling: is er een datalek?

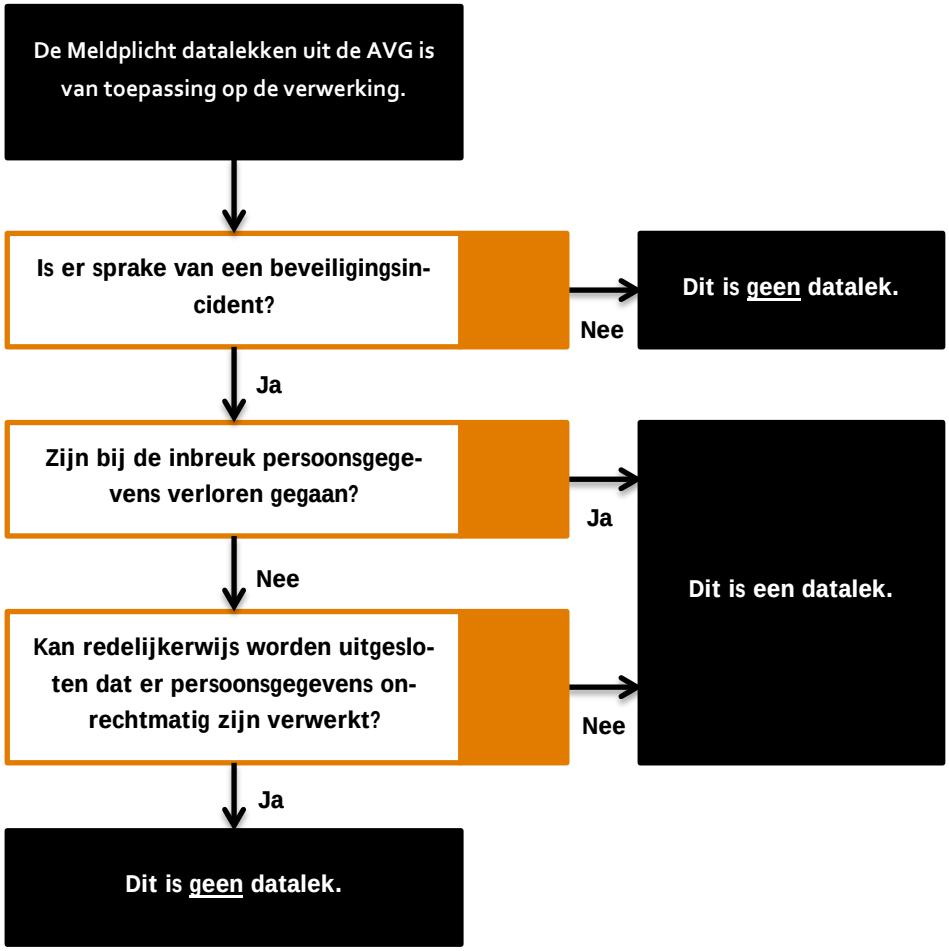
Beveiligingsincident: een inbreuk op de beveiliging die *niet* leidt tot vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens.

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

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 Autoriteit Persoonsgegevens 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



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.

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.

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.

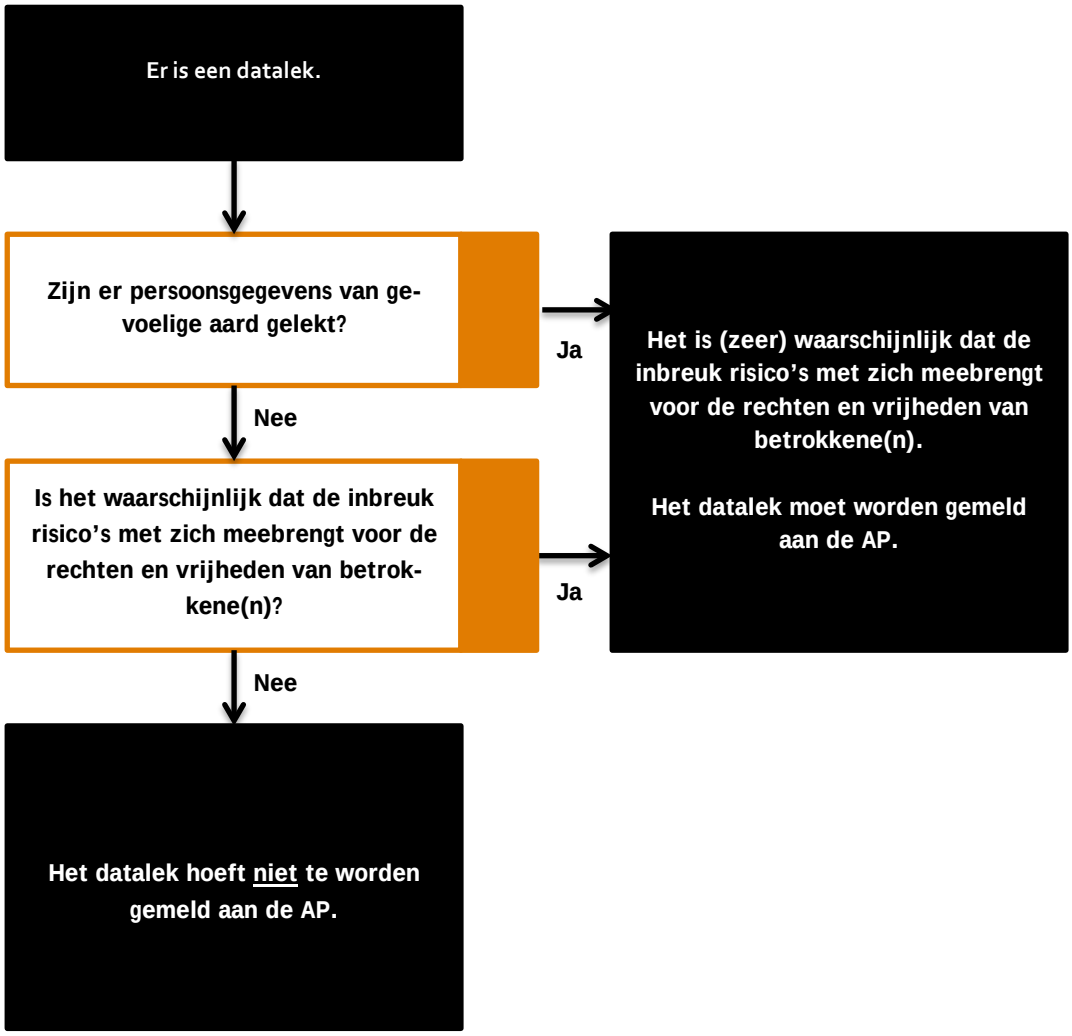
Voorbeeld 12

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.

Melding datalek aan Autoriteit persoonsgegevens

Indien wordt geoordeeld door het IRT en de Functionaris Gegevensbescherming dat er sprake is van een datalek, dient vervolgens door de Functionaris Gegevensbescherming bepaald te worden of het datalek aan de AP dient te worden gemeld. De meldingsplicht aan de Autoriteit Persoonsgegevens 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.



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.[3]
- *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.

3 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.

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.

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).

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.

Onverwijlde melding aan Autoriteit persoonsgegevens

Indien melding van het datalek aan de Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens, dan dient de Functionaris Gegevensbescherming deze melding onverwijld te doen aan de Autoriteit Persoonsgegevens.

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. 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 Autoriteit Persoonsgegevens 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 Functionaris Gegevensbescherming) een melding bij de Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens wordt gemeld, dan dient desgevraagd te kunnen worden gemotiveerd aan de Autoriteit Persoonsgegevens 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 Privacy Officer 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.

Het College van Bestuur is eindverantwoordelijk voor een onverwijlde en tijdige melding aan de AP.

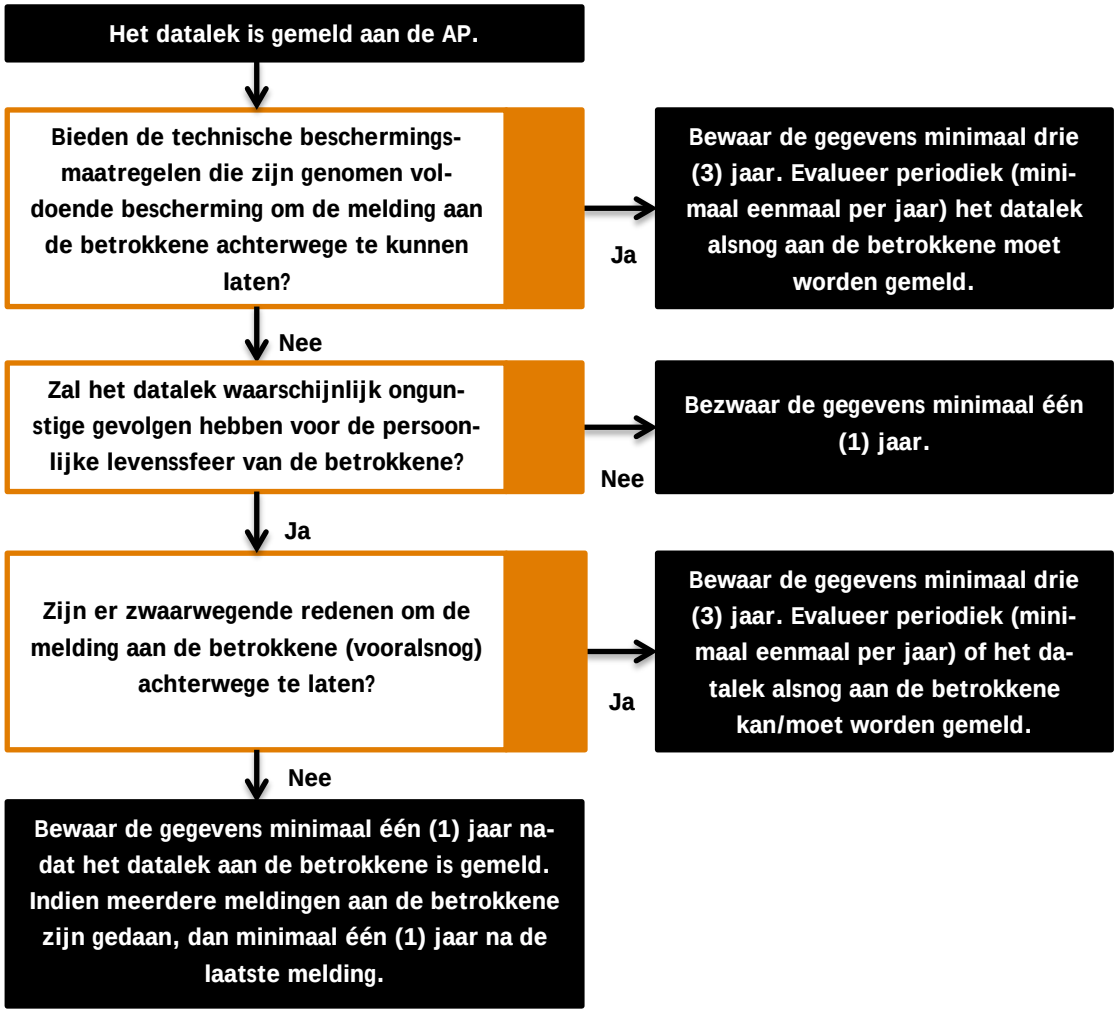
Wijze van melding aan Autoriteit persoonsgegevens

Het datalek zal door de Functionaris Gegevensbescherming worden gemeld bij de Autoriteit Persoonsgegevens. Dit gebeurt digitaal. De Functionaris Gegevensbescherming behoudt een afschrift van de melding. De Bestuurssecretaris is eindverantwoordelijk voor de inhoud van de melding. In geval een melding aanleiding geeft tot nadere actie door de Autoriteit Persoonsgegevens, zal de Bestuurssecretaris als contactpersoon functioneren.

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). 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 Autoriteit Persoonsgegevens 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. 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 bovenstaande schema biedt u een beslismodel voor het vaststellen van de bewaartermijnen van geregistreerde datalekken.

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.

BIJLAGE IV 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 Begripsbepaling

1. Artikel 1 van het Privacyreglement is van overeenkomstige toepassing.
2. beveiligingsincident: een inbreuk op de beveiliging die mogelijk leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
3. datalek: een inbreuk op de beveiliging die wel leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;

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 Functionaris Gegevensbescherming of Privacy Officer 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 Privacy Officer.

Artikel 5 Persoonsgegevens

Persoonsgegevens zijn niet alleen gegevens zoals naam, adres, woonplaats of BSN-nummer. 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;
- medische gegevens;
- dyslexie;
- betalingsachterstanden;
- gegevens over gezinssituatie;
- geloof;
- ras;
- studieresultaten;

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.

<u>Niet bewuste incidenten</u>
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 een laptop;
- door haperende beveiliging (technische storing) zijn mogelijk persoonsgegevens van leerlingen ingezien door onbevoegden;
- de ruimte op school met daarin de fysieke leerling dossiers 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 e-mailadressen 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: SomToday) voor zover het persoonsgegevens betreft van personeel of (ouder(s) en/of verzorger(s) van) leerlingen van de school.

<u>Bewuste incidenten</u>
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 verwerker van de school (bijvoorbeeld: SomToday) 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 Privacy Officer via privacy@sovop.nl.