wille donker
advocaten

VGS
vereniging voor gereformeerd schoolonderwijs

Privacyreglement [naam stichting]

Vastgesteld door het College van Bestuur: [datum]
Instemming oudergeleding (G)MR (artikel 14 lid 2 sub f WMS): [datum]
Instemming personeelsgeleding (G)MR (artikel 12 lid 1 sub m en sub n WMS): [datum]
Inwerkingtreding: [datum]

Inhoudsopgave

e. De gegevens genoemd in artikel 5.1.3. onder j. en n. worden bewaard op een afgesloten, slechts voor bevoegden toegankelijk deel van de server van het bevoegd gezag (**bijlage II**);

f. De server van het bevoegd gezag staat geplaatst in [adres];

g. In het kader van onderwijsdoeleinden wordt tevens gebruik gemaakt van andere servers dan die van de Stichting en de door haar gecontracteerde bewerkers (sociale media en software-applicaties die leerlingen op hun eigen ICT-middelen downloaden). De Stichting maakt van deze servers uitsluitend gebruik met het oog op onderwijskundige doeleinden en - in het geval van leerlingen van 16 jaar en jonger - slechts na voorafgaande schriftelijke toestemming van hun ouders.

5.2. Personeel

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

a. het aangaan van de arbeidsovereenkomst (openbaar onderwijs: het aanstellen van de medewerker) (artikel 8b Wbp);

b. het vaststellen van salarisaanspraken en arbeidsvoorwaarden (artikel 8b Wbp);

c. het (laten) uitbetalen van salaris, de afdracht van belastingen en premies (artikelen 8b en 8c Wbp);

d. de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde (artikel 8b Wbp);

e. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen (artikel 8b Wbp);

f. het verlenen van ontslag (artikel 8b Wbp);

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 verantwoordelijke is verbonden (artikel 8b Wbp);

h. het geven van leiding aan de werkzaamheden van betrokkene (artikel 8b Wbp);

i. het verstrekken van de bedrijfsmedische zorg voor betrokkene en het kunnen nakomen van re-integratieverplichtingen bij verzuim (artikel 8c Wbp);

j. het toegang verlenen tot het schoolnetwerk (artikel 8b Wbp);

k. het regelen van en de controle van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband (artikel 8b Wbp);

l. de verkiezing van de leden van een bij wet geregeld medezeggenschapsorgaan (artikel 8c Wbp);

m. het behandelen van geschillen (artikel 8b Wbp);

n. de behandeling van personeelszaken, anders dan genoemd onder a. tot en met m. (artikel 8b Wbp);

o. de organisatie of het geven van het onderwijs en de begeleiding van docenten (artikel 8f Wbp);
p. het laten uitoefenen van accountantscontrole en het laten vaststellen van aanspraken op bekostiging (artikel 8c en artikel 8f Wbp);
q. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 8f Wbp).

5.2.2. Grondslagen van de gegevensverwerking:
De verwerking van de persoonsgegevens ten behoeve van de doelen genoemd in artikel 5.2.1. vindt plaats op basis van de grondslagen zoals aangeduid tussen de haakjes achter het betreffende doel in artikel 5.2.1. Het betreft één of meerdere van de grondslagen genoemd in artikel 8 (zie **bijlage I**).

5.2.3. 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 en geboorteplaats;
f. gegevens als bedoeld onder a., van de ouders, voogden of verzorgers van minderjarige werknemers;
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;

Artikel 9. Bewaartermijnen

9.1. Voor de gegevens in het leerlingdossier geldt dat deze gegevens gedurende [twee jaar] nadat de desbetreffende leerling van de school is uitgeschreven worden bewaard, tenzij ze wegens een wettelijke bewaarplicht langer moeten worden bewaard. Voor de gegevens opgenomen in de leerlingadministratie geldt dat deze vijf jaar nadat de desbetreffende leerling van de school is uitgeschreven dienen te worden bewaard, tenzij ze wegens een wettelijke bewaarplicht langer moeten worden bewaard.

9.2. De persoonsgegevens van medewerkers worden verwijderd twee jaar nadat het dienstverband is geëindigd, tenzij andere wettelijke bepalingen het langer bewaren van (een aantal van) deze gegevens in een (geautomatiseerde) persoonsregistratie vereisen.

9.3. De persoonsgegevens van sollicitanten worden verwijderd op een daartoe strekkend verzoek van betrokkenen en in ieder geval vier weken nadat de sollicitatieprocedure is geëindigd, tenzij de persoonsgegevens met toestemming van betrokkene gedurende een jaar na beëindiging van de sollicitatieprocedure worden bewaard.

9.4. De persoonsgegevens van oud-medewerkers worden verwijderd op een daartoe strekkend verzoek van betrokkenen en zodra de verantwoordelijke bekend geworden is met hun overlijden.

9.5. De persoonsgegevens van oud-leerlingen worden verwijderd op een daartoe strekkend verzoek van betrokkenen en zodra de verantwoordelijke bekend geworden is met hun overlijden.

9.6. De persoonsgegevens van leden van de Raad van Toezicht worden verwijderd twee jaar nadat de benoemingstermijn is geëindigd, tenzij andere wettelijke bepalingen het langer bewaren van (een aantal) van deze gegevens in een (geautomatiseerde) persoonsregistratie vereisen. Hierbij wordt aansluiting gezocht bij de bewaartermijnen die worden gehanteerd voor de persoonsgegevens van medewerkers.

9.7. De persoonsgegevens van bezoekers worden verwijderd uiterlijk zes maanden na de datum van het bezoek, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.

9.8. Onverminderd het bepaalde in artikel 9.1 t/m 9.7 geldt dat voor zover van de in deze leden genoemde betrokkenen videobeelden zijn gemaakt in het kader van beveiliging en toezicht,

Artikel 10. Beveiliging en geheimhouding

10.1. De verantwoordelijke draagt zorg voor passende technische en organisatorische maatregelen ter voorkoming van verlies of onrechtmatige verwerking van persoonsgegevens.

10.2. De wijze van beveiliging van beveiliging van de persoonsgegevens is beschreven en toegelicht in **bijlage VI**.

10.3. Tevens hanteert de Stichting een protocol voor het gebruik van ICT, e-mail, internet, en sociale media (**bijlage XVI**). Deze regeling geeft de wijze aan waarop binnen [naam stichting] 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.

10.4. Deze maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

10.5. Indien sprake is van digitale verwerking van persoonsgegevens zal de FG via een coderingsbeveiliging de verschillende functionarissen, als bedoeld in artikel 6, toegang geven tot bepaalde gedeelten van de persoonsgegevens of tot alle persoonsgegevens al naar gelang hun werkzaamheden dit vereisen.

10.6. Een ieder die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan en tekent de geheimhoudingsverklaring die is opgenomen in **bijlage VII**. 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 12. Beveiligingsincidenten

12.1. Indien zich binnen de organisatie van verantwoordelijke of bij een door de verantwoordelijke ingeschakelde bewerker een beveiligingsincident voordoet, waarbij een aanzienlijke kans bestaat op verlies of onrechtmatige verwerking van persoonsgegevens die door verantwoordelijke worden verwerkt, dan wel dit verlies of onrechtmatige verwerking zich daadwerkelijk voordoet, zal de verantwoordelijke daarvan melding doen bij de Autoriteit Persoonsgegevens en indien voorgeschreven op grond van de wet tevens aan betrokkenen.

12.2. Het vaststellen of sprake is van een datalek en of melding daarvan moet worden gedaan bij de Autoriteit Persoonsgegevens vindt plaats conform de voorschriften en werkwijzen die zijn opgenomen in het handboek en protocol Datalekken (**bijlage IX**).

Artikel 16. De bewerker

16.1. De bewerkers zijn derden die op basis van een overeenkomst voor of namens het bevoegd gezag gegevens verwerken. Voor het bevoegd gezag zijn dit de organisaties en instellingen die zijn vermeld in **bijlage X**.

16.2. De bewerker verwerkt de gegevens op de wijze zoals overeengekomen in een bewerkersovereenkomst (**bijlage XI**), tenzij de bewerker die gegevens verwerkt bij het gebruik van leermiddelen, toetsen, school- en leerlinginformatiemiddelen (zoals gedefinieerd in artikel 1 sub f., sub g. en sub h. van de Model Bewerkersovereenkomst behorend bij het Convenant Digitale Onderwijsmiddelen). In dat geval verwerkt de bewerker de gegevens zoals voorgeschreven in de Model Bewerkersovereenkomst met inachtneming van de aanvullingen en wijzigingen zoals opgenomen in bijlage 3 (**bijlage XII**)

16.3. De bewerker 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 bewerkersovereenkomst.

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

Bijlagenoverzicht

Bijlage I	Wet bescherming persoonsgegevens
Bijlage II	Toegang tot persoonsregistratie
Bijlage III	Toestemmingsformulier oud-personeelsleden
Bijlage IV	Toestemmingsformulier oud-leerlingen
Bijlage V	Bewaartermijn personeelsdossier
Bijlage VI	Beveiligingsmaatregelen
Bijlage VII	Geheimhoudingsverklaring
Bijlage VIII	Uitvoering meldingsplicht bij Autoriteit Persoonsgegevens
Bijlage IX	Handboek en protocol datalekken
Bijlage X	Bewerkers die voor het bevoegd gezag persoonsgegevens verwerken
Bijlage XI	Bewerkersovereenkomst algemeen
Bijlage XII	Bewerkersovereenkomst digitale leermiddelen
Bijlage XIII	Modelantwoord op een verzoek ex artikel 35 Wbp (leerlingen)
Bijlage XIV	Modelantwoord op een verzoek ex artikel 35 Wbp (personeel)
Bijlage XV	Privacy statement bezoekers website
Bijlage XVI	Protocol voor het gebruik van e-mail, internet, en sociale media
Bijlage XVII	Protocol gebruik van camera- en videobeelden

HANDBOEK DATALEKKEN
[naam stichting]

Inwerkingtreding: [datum]

Inhoudsopgave

1. Inleiding

Per 1 januari 2016 is als gevolg van een wetswijziging de verplichting ingevoerd voor een verantwoordelijke (in dit verband: de school) om een datalek te melden aan de Autoriteit persoonsgegevens (AP) en mogelijk ook aan de betrokkenen. 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 verantwoordelijke dient te worden aangemerkt en welke afwegingen zij dient te maken om vast te stellen of daadwerkelijk sprake is van een datalek dat dient te worden gemeld aan de AP en/of de betrokkene.

Dit handboek is gebaseerd op het bepaalde in artikel 34a Wet bescherming persoonsgegevens (Wbp), welke bepaling als volgt luidt:

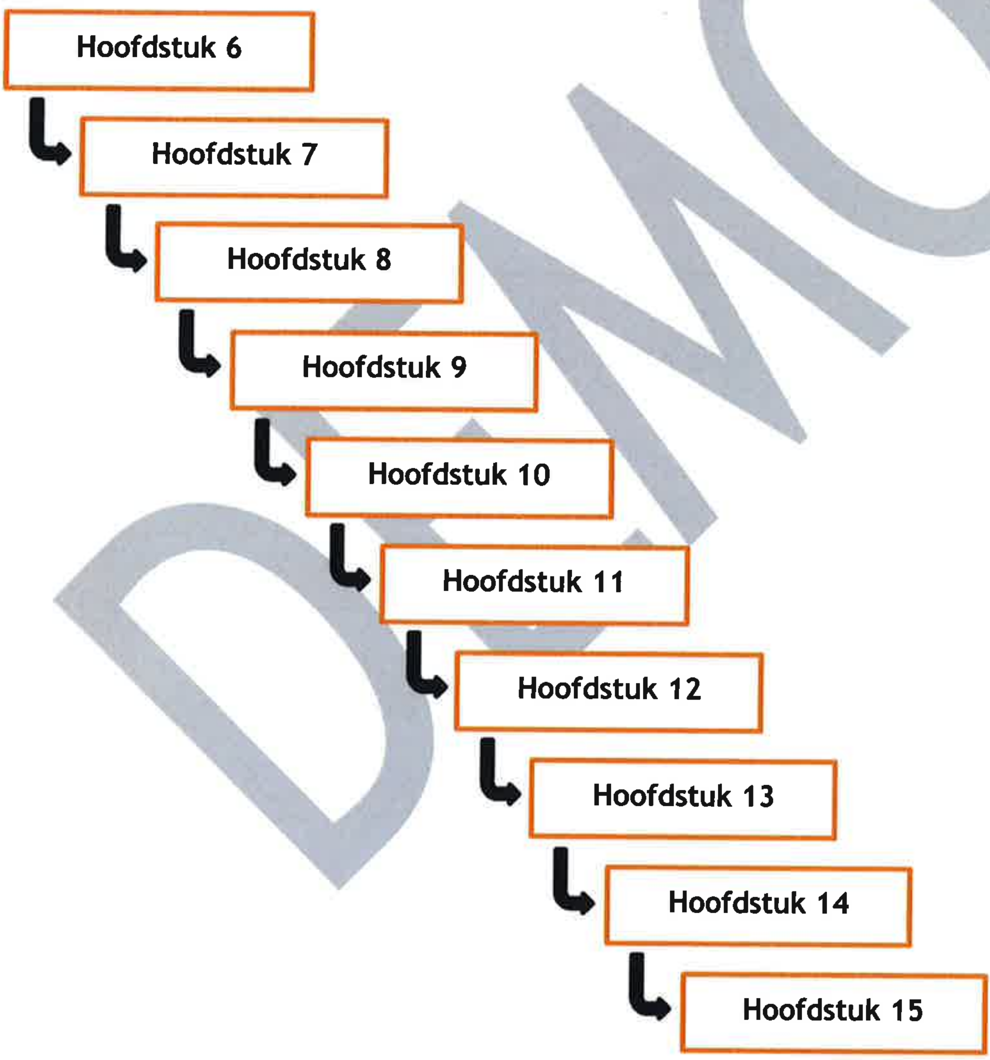
1. *De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.*
2. *De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.*
3. *De kennisgeving aan het College en de betrokkene omvat in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.*
4. *De kennisgeving aan het College omvat tevens een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.*
5. *De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.*
6. *Het tweede lid is niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.*
7. *Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het College, indien het van oordeel is dat inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog een kennisgeving doet.*
8. *De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.*

9.	*Dit artikel is niet van toepassing indien de verantwoordelijke in zijn hoedanigheid als aanbieder van een openbare elektronische communicatiedienst een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet.*
10.	*Het tweede en zevende lid zijn niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.*
11.	*Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving.*

De inhoud van dit handboek is tevens mede gebaseerd op hetgeen opgenomen in de Kamerstukken behorend bij wetsvoorstel 33 662, de 'Beleidsregels voor toepassing van artikel 34a van de Wbp' d.d. 8 december 2015 van de AP en de 'Boetebeleidsregels Autoriteit persoonsgegevens 2016' d.d. 15 januari 2016.

2. Werkwijze

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



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

BIJLAGE 1 PROTOCOL BEVEILIGINGSINCIDENTEN

Artikel 1. Doel van dit protocol

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

Artikel 2. Begripsbepalingen

1.	personeel(slid):	het personeel als bedoeld in artikel 1 onder @ van het Handboek Datalekken;
2.	beveiligingsincident:	is een inbreuk op de beveiliging waarbij <u>mogelijk</u> persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking;
3.	beveiligingslek:	is een inbreuk op de beveiliging waarbij <u>geen</u> persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking
4.	datalek:	is een inbreuk op de beveiliging waarbij <u>wel</u> persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking
5.	persoonsgegevens:	de gegevens als bedoeld in artikel 4;
6.	FG:	de functionaris gegevensbescherming, zijnde heer/mevrouw: @, [@mailadres] en [@telefoonnummer];

Artikel 3. Meldplicht datalekken

Per 1 januari 2016 dient een verantwoordelijke (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 is sprake indien er persoonsgegevens verloren gaan of onrechtmatig worden verwerkt en dit leidt tot (de aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

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 mail of telefonisch te melden aan de FG ongeacht het tijdstip van de dag. Deze melding zal zo concreet mogelijk zijn. Het personeelslid neemt daarbij de inhoud van dit protocol in acht.

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

Artikel 5. Persoonsgegevens

Wat zijn persoonsgegevens? Dit zijn niet alleen gegevens zoals naam, adres, woonplaats of 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;
- gegevens met betrekking tot gezondheid;
- dyslexie;
- betalingsachterstanden;
- gegevens over gezinssituatie;
- geloof;
- ras;
- studieresultaten;
- etc.

Artikel 6. Soorten beveiligingsincidenten

Er zijn verschillende soorten beveiligingsincidenten. Sommige beveiligingsincidenten zijn het gevolg van menselijke fouten, onoplettendheid of technisch falen. Deze beveiligingsincidenten worden niet bewust gecreëerd. Veel beveiligingsincidenten worden echter bewust gecreëerd.
Niet bewuste incidenten
Bij niet bewuste beveiligingsincidenten gaat het om incidenten die niet met opzet worden gecreeerd. Te denken valt aan:

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

Indien zich een dergelijk incident - of soortgelijkend incident - voor doet, is er sprake van een beveiligingsincident en dient het personeelslid dit te melden aan de FG.