Protocol beveiligingsincidenten

Artikel 1. Doel van dit protocol

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

Artikel 2. Begripsbepalingen

1.	personeel(slid):	a) de bij LiemersNovum benoemde directeur, adjunct-directeur, leraar en overige medewerkers benoemd in een andere functie dan het geven van onderwijs b) onder a bedoelde medewerker die zonder benoeming is tewerkgesteld;
2.	beveiligingsincident:	is een inbreuk op de beveiliging die mogelijk leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
3.	datalek:	is een inbreuk op de beveiliging die wel leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
4.	persoonsgegevens:	de gegevens als bedoeld in artikel 1 van het Privacyreglement;
5.	FG:	de functionaris gegevensbescherming, zijnde: Dick Stam, dick.stam@liemersnovum.nl.

Artikel 3. Meldplicht datalekken

Sinds 1 januari 2016 dient een verwerkingsverantwoordelijke (in dit geval Stichting LiemersNovum) 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 dat 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 stichting 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 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 dit toch meldt aan de FG.

Artikel 5. Persoonsgegevens

Wat zijn persoonsgegevens? Dit zijn niet alleen gegevens zoals naam, adres, woonplaats of BSN. Deze gegevens worden aangeduid als direct identificerende gegevens. Daarnaast zijn er ook indirect identificerende gegevens. Dit zijn gegevens die iets zeggen over een natuurlijk persoon omdat zij gekoppeld kunnen worden aan een direct persoonsgegeven. Indien kan worden achterhaald om welke natuurlijke persoon het gaat, is er sprake van een persoonsgegeven. Het kan dus onder andere gaan om:

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

Artikel 6. Soorten beveiligingsincidenten

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

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

- het laten liggen van een laptop, tablet, smartphone of papieren dossier in de trein;
- het verliezen van een USB-stick[1], mobiele telefoon of bijvoorbeeld laptop;
- door haperende beveiliging (technische storing) zijn mogelijk persoonsgegevens van leerlingen ingezien door onbevoegden;

[1] Binnen LiemersNovum is de afspraak dat (bestanden met) persoonsgegevens niet op een USB stick worden gezet. Dit betekent dat bij het verlies van een USB stick geen persoonsgegevens verloren gaan of onrechtmatig kunnen worden verwerkt. Bij verlies van een USB-stick kan dus geen sprake zijn van een datalek, mogelijk wel van een beveiligingsincident.

- 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 hiervoor genoemde situaties die zich voordoet bij een verwerker van de school (bijvoorbeeld: de uitgever van digitale leermiddelen) 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 hiervoor genoemde situaties die zich voordoet bij een bewerker van de school (bijvoorbeeld: de uitgever van digitale leermiddelen) voor zover het persoonsgegevens betreft van personeel of (ouder(s) en/of verzorger(s) van) leerlingen van de school.

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