Bijlage XIII.a Bijlagen 1-5 bij Handboek Datalekken

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 hoofdstuk 3 van het Handboek Datalekken;
2.	beveiligingsincident:	is een inbreuk op de beveiliging die mogelijk leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
3.	datalek:	is een inbreuk op de beveiliging die wel leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
4.	persoonsgegevens:	de gegevens als bedoeld in artikel 1 van het Privacyreglement;
5.	FG:	de functionaris gegevensbescherming, functionarisgegevensbescherming@calvijncollege.nl en 0113-21 10 20.

Artikel 3. Meldplicht datalekken

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

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

Artikel 4. Meldingsplicht personeel

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

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

Artikel 5. Persoonsgegevens

Wat zijn persoonsgegevens? Dit zijn niet alleen gegevens zoals naam, adres, woonplaats of 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 gecreëerd. Te denken valt aan:

- het laten liggen door van een laptop, tablet, smartphone of papieren dossier in de trein;
- het verliezen van een USB-stick, mobiele telefoon of bijvoorbeeld laptop;
- door haperende beveiliging (technische storing) zijn mogelijk persoonsgegevens van leerlingen ingezien door onbevoegden;
- de ruimte op school met daarin de fysieke leerlingdossiers heeft per ongeluk niet op slot gezeten voor een bepaalde periode;
- een docent heeft per ongeluk onbeheerd zijn laptop in de klas laten staan met daarop een memo-sticker met zijn inlognaam en wachtwoord;

- het verzenden door een medewerker van e-mail met vertrouwelijke gegevens aan de verkeerde ontvanger;
- het verzenden van een e-mail aan meerdere ontvangers die elkaars emailadressen niet kennen (zonder gebruik te maken van de bcc-optie);
- het crashen van een harde schijf met daarop persoonsgegevens;
- brand in een serverruimte of archiefruimte van de school;
- één van de hier voor genoemde situaties zich voordoet bij een verwerker van de school (bijvoorbeeld: de uitgever van digitale leermiddelen en Magister) voor zover het persoonsgegevens betreft van personeel of (ouder(s) en/of verzorger(s) van) leerlingen van de school.

Bewuste incidenten

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

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

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

Bijlage 2 Incident Response Team

Het Incident Response Team (IRT) bestaat uit de volgende vaste leden:

1) Voorzitter bestuur: Jan Bakker, bak@calvijncollege.nl
2) FG: Ad Verwijs, functionarisgegevensbescherming@calvijncollege.nl
3) Hoofd van de ICT-afdeling: Ad Verwijs, vrs@calvijncollege.nl

Zo nodig wordt het IRT aangevuld met:

4) een forensisch IT-deskundige
5) een juridisch adviseur
6) de communicatieadviseur: Peter Smit, smp@calvijncollege.nl

Bijlage 3 Formulier gegevens datalek

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

Gegevens over het datalek

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

c) Blootstelling aan (identiteits)fraude
d) Blootstelling aan spam of phishing
e) Anders, namelijk [vul aan]

Vervolgacties naar aanleiding van het datalek

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

Technische beschermingsmaatregelen

9) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)
   a) Ja
   b) Nee
   c) Deels, namelijk: [vul aan]
10) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als de School bij vraag 24 gekozen heeft voor optie a of optie c. Als de School gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Bijlage 4 Meldformulier

Gegevens over het datalek

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

Vervolgacties naar aanleiding van het datalek

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

Technische beschermingsmaatregelen

9) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)
   a) Ja
   b) Nee
   c) Deels, namelijk: [vul aan]
10) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als de School bij vraag 24 gekozen heeft voor optie a of optie c. Als de School gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Vervolgacties naar aanleiding van het datalek

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

Inlichten van de betrokkenen

12) Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (Kies een van de volgende opties.)
   a) Ja
   b) Nee
   c) Nog niet bekend
13) Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord. Kies een van de volgende opties en vul waar nodig aan.)
   a) Ik heb het datalek aan de betrokkenen gemeld op [datum]
   b) Ik ga het datalek aan de betrokkenen melden op [datum]
   c) Nog niet bekend
14) Wat is de inhoud van de melding aan de betrokkenen? (Letterlijke weergave, beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)
15) Hoe veel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)
16) Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

17) Waarom ziet u af van het melden van het datalek aan de betrokkenen? (Beantwoord deze vraag als u vraag 18 met nee hebt beantwoord. Kies een van de onderstaande opties en vul waar nodig aan.)
    a) De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten.
    b) Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: [vul aan]
    c) Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: [vul aan]
    d) Anders, namelijk: [vul aan]

Technische beschermingsmaatregelen

18) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)
    a) Ja
    b) Nee
    c) Deels, namelijk: [vul aan]
19) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij vraag 24 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Internationale aspecten

20) Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)
    a) Ja
    b) Nee
    c) Nog niet bekend
21) Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
    a) Ja, namelijk: [vul aan]
    b) Nee

Vervolgmelding

22) Is naar uw mening deze melding compleet? (Kies een van de onderstaande opties.)
    a) Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
    b) Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

Bijlage 5 Registratie Datalekken Calvijn College

Korte omschrijving van het lek:	
Wanneer vond het lek plaats?	
Wat is er met de gegevens gebeurd? (verloren gegaan/door een onbevoegde ingezien/ gekopieerd/gewijzigd)	
Van wie (welke groepen) zijn gegevens gelekt?	
Om hoeveel personen gaat het?	
Om welke persoonsgegevens gaat het?	
Wat zijn de (mogelijke) gevolgen van de inbreuk (bijvoorbeeld risico op identiteitsfraude of reputatieschade)	
Welke maatregelen zijn genomen naar aanleiding van het lek? (schadebeperking)	
Welke maatregelen zijn genomen om te zorgen dat het niet nog een keer kan gebeuren?	

Korte omschrijving van het lek:	
Wanneer vond het lek plaats?	
Wat is er met de gegevens gebeurd? (verloren gegaan/door een onbevoegde ingezien/ gekopieerd/gewijzigd)	
Van wie (welke groepen) zijn gegevens gelekt?	
Om hoeveel personen gaat het?	
Om welke persoonsgegevens gaat het?	
Wat zijn de (mogelijke) gevolgen van de inbreuk (bijvoorbeeld risico op identiteitsfraude of reputatieschade)	
Welke maatregelen zijn genomen naar aanleiding van het lek? (schadebeperking)	
Welke maatregelen zijn genomen om te zorgen dat het niet nog een keer kan gebeuren?	

Korte omschrijving van het lek:	
Wanneer vond het lek plaats?	
Wat is er met de gegevens gebeurd? (verloren gegaan/door een onbevoegde ingezien/ gekopieerd/gewijzigd)	
Van wie (welke groepen) zijn gegevens gelekt?	
Om hoeveel personen gaat het?	
Om welke persoonsgegevens gaat het?	
Wat zijn de (mogelijke) gevolgen van de inbreuk (bijvoorbeeld risico op identiteitsfraude of reputatieschade)	
Welke maatregelen zijn genomen naar aanleiding van het lek? (schadebeperking)	
Welke maatregelen zijn genomen om te zorgen dat het niet nog een keer kan gebeuren?	