PROCEDURE MELDPLICHT DATALEKKEN

Procesgang rondom (mogelijke) datalekken in de Openbare Scholengemeenschap Reigersbos

Documentstatus:

Versie: vastgesteld door CvB en MR op 19 juli 2017

Inhoud

1. Doel

Met ingang van 1 januari 2016 is de Wet bescherming persoonsgegevens (Wbp) gewijzigd. Sindsdien geldt een meldplicht voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken onverwijld moeten melden aan de Autoriteit Persoonsgegevens (AP), en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.
De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt, moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt.

Deze procedure beschrijft hoe te handelen binnen SGR indien er sprake is van een datalek of wanneer een datalek vermoed wordt. De meldplicht is eveneens van toepassing op SGR, als het datalek bij een derde is ontstaan, bijvoorbeeld een bewerker van persoonsgegevens van SGR zoals Afas of Driessen.
Deze procedure is mede gebaseerd op de beleidsregels van de AP inzake de meldplicht datalekken in de Wet bescherming persoonsgegevens.

Per gemeld datalek behoudt het bestuur van SGR de vrijheid te beoordelen of de procedure gevolgd kan worden, danwel afwijking van deze procedure gerechtvaardigd is.

Het doel van deze procedure is vast te leggen, welke stappen genomen moeten worden door SGR bij het vermoeden van of kennis nemen van een incident dat (mogelijk) aangemerkt kan worden als een datalek.
Het volgende resultaat wordt hiermee nagestreefd:

- het steeds volgen van een eenduidige procedure;
- het zorgvuldig waarborgen van de belangen van SGR, het individu dan wel een ander bedrijf dat betrokken is bij het incident, zijnde (mogelijk)datalek;
- het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident;
- het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen;
- het realiseren van een voldoende en eenduidige interne en op verzoek externe verantwoording over de afhandeling van een incident, zijnde (mogelijk) datalek.

In de procedurebeschrijving zijn de te doorlopen stappen verwoord.

2. Definities

AP
Autoriteit Persoonsgegevens, de nieuwe naam van het College Bescherming Persoonsgegevens (CBP) m.i.v. 1-1-2016.

Bestand
Elk gestructureerd geheel van persoonsgegevens (op papier als digitaal ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze), dat

volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen (artikel 1c, Wbp).

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft (artikel 1f, Wbp).

Beveiligingslek
Een inbreuk op de beveiliging (zoals bedoeld in artikel 34a, lid 1, Wbp) waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking; er is dan geen sprake van een datalek.

Bewerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 1e, Wbp).

Datalek
Een inbreuk op de beveiliging (zoals bedoeld in artikel 34a, lid 1, Wbp) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 13, Wbp)bescherming moesten bieden.

Datalekken Commissie
Een door de Manager Informatieveiligheid tijdelijk ingestelde onderzoekscommissie, die zorgdraagt voor een onderzoek en over de uitkomsten rapporteert aan het bestuur van SGR.

Derden
De bij het incident betrokken externe partij, anders dan betrokkene. Bv. een bewerker van persoonsgegevens t.b.v. SGR.

Genodigden
Interne betrokkenen die uitgenodigd zijn bij de bespreking(en) van het incident bij SGR.

CG
Coördinator Gegevensbescherming. Binnen SGR is dat de financieel stafmedewerker.

Incident
Een mogelijk beveiligingsincident, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder datalek is een incident, niet ieder incident is een datalek.

ISO
Information Security Officer. Binnen SGR is dat een taak die is neergelegd bij de ICT-beheerder.

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon Wbp (artikel 1a, Wbp).

Wbp
Wet bescherming persoonsgegevens.

Verantwoordelijke
De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of

tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1d, Wbp).

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1b, Wbp).

Manager Informatieveiligheid
De manager, die vanuit de portefeuille Informatieveiligheid belast is met de interne coördinatie van de procedure Meldplicht Datalekken. Binnen SGR is dat belegd bij het hoofd bedrijfsbureau.

3. Toepassingsgebied

Deze procedure wordt gehanteerd bij het melden en afhandelen van (mogelijke) datalekken binnen SGR, dan wel van (mogelijke) datalekken die buiten SGR hebben plaatsgevonden, doch waarvoor SGR als Verantwoordelijke wel de eindverantwoordelijkheid draagt (bv. bij een Bewerker).

4. Werkwijze

Ten behoeve van het totaal overzicht is een processchema opgesteld. Vervolgens wordt specifieke informatie per processtap over de te verrichten activiteiten en bijbehorende verantwoordelijkheden en bevoegdheden uitgewerkt.

(processchema volgt na vaststelling procedure)

4.1. Identificeren van een datalek

De medewerker[1] die een (mogelijk) datalek constateert, meldt dit incident per omgaande bij zijn organisatorisch hoofd, en deze meldt het incident per omgaande aan de Manager Informatieveiligheid.
Een medewerker is te allen tijde bevoegd zelfstandig een melding te doen aan de Manager Informatieveiligheid bij gebreke van een melding aan de Manager Informatieveiligheid anderszins. De procedure Meldplicht Datalekken wordt dan gestart.

4.2. Beoordeling aard/ernst incident; datalek ja/nee

- De Manager Informatieveiligheid draagt, in samenspraak met de CG, zo spoedig mogelijk zorg voor volledige en juiste informatie zoals opgenomen in Bijlage 1 'Formulier t.b.v. melding datalek'.
- Op basis van de verkregen informatie en bij vermoeden van een datalek wordt in overleg tussen het bestuur van SGR, het hoofd bedrijfsbureau, de Manager Informatieveiligheid en de ISO zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een datalek.

[1]Dit kan ook een medewerker van een Bewerker zijn, die dit vervolgens meldt aan diens opdrachtgever binnen SGR

- In dit overleg wordt tevens beoordeeld of er per direct maatregelen genomenmoeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen. Zo nodig kan juridisch en communicatie- advies gevraagd worden
- Tevens kan wordt beoordeeld of het datalek (mogelijk) meldingsplichtig is voor de politie in geval van vermoeden van een strafbaar feit (zie ook hierna onder 4.3).
- De beoordeling of er sprake is van een incident, dat gemeld moet worden aan de AP kan tot stand komen met behulp van de schema's te vinden in de beleidsregels "Meldplicht datalekken in de Wet bescherming persoonsgegevens" van de AP (zie Bijlage 2).
  Bij de beoordeling spelen o.a. een rol:
  - is er sprake van verlies van persoonsgegevens; dit houdt in dat SGR deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan;
  - is er sprake van onrechtmatige verwerking van persoonsgegevens; hier onder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan;
  - is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging;
  - kan redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot onrechtmatige verwerking heeft geleid;
  - zijn er persoonsgegevens van gevoelige aard gelekt:
    § bijzondere persoonsgegevens conform artikel 16 Wbp;
    § gegevens over de financiële of economische situatie van de betrokkene;
    § gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
    § gebruikersnamen, wachtwoorden en andere inloggegevens;
    § gegevens die kunnen worden gebruikt voor (identiteits)fraude;
  - leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen; betrek hierbij factoren als
    § de omvang van de verwerking; gaat het om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen;
    § de impact van verlies of onrechtmatige verwerking;
    § het delen van de persoonsgegevens binnen (zorg)ketens; dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten kunnen optreden;
    § betrokkenheid van kwetsbare groepen; denk aan verstandelijk gehandicapten;
    - In geval geoordeeld wordt, dat sprake is van een (mogelijk) datalek, wordt tevens het communicatietraject richting betrokkene(n) en indien van toepassing de bewerker besproken;
    - In geval dat het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. Melding aan de AP is dan niet aan de orde. Wel kan in het overleg besloten worden, dat het zinvol is om het beveiligingslek te onderzoeken om herhaling te voorkomen.

4.3. Melden aan de Autoriteit Persoonsgegevens

- Het bestuur van SGR of op diens verzoek de CG verzorgt de tijdige elektronische melding bij de AP volgens het online meldingsformulier van de AP met inachtneming van de richtlijnen van de AP ter zake. Met tijdige melding wordt bedoeld onverwijld, zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek.
  De Manager Informatieveiligheid draagt, in samenspraak met de CG, zorg voor volledige en juiste informatie zoals opgenomen in bijlage 1 "formulier t.b.v. melding datalek" aan het

bestuur van SGR op grond waarvan feitelijk gemeld kan worden. Het bestuur van SGR of op diens verzoek de CG fungeert als contactpersoon inzake de communicatie naar de AP. Dit geldt ook ingeval nog niet duidelijk is dat het incident een datalek is. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het incident de melding aan te vullen dan wel in te trekken.

- Het bestuur van SGR is eindverantwoordelijk, de Manager Informatieveiligheid is gedelegeerd regievoerder over de interne afhandeling van het (mogelijke) datalek in al zijn facetten, de CG draagt zorg voor de externe afhandeling, waaronder het AP, betrokkenen en bewerker.
- Het direct betrokken (afdelings) management draagt ervoor zorg dat de bij het incident betrokken medewerkers worden geïnformeerd indien dit leden van het onderwijzend personeel zijn. Het hoofd bedrijfsbureau vervult deze taak als de betrokken medewerkers leden van het onderwijsondersteunend personeel zijn. De betrokken medewerkers worden door deze leidinggevenden verzocht zo snel mogelijk een eigen verslag op te stellen over de toedracht van het incident. Deze schriftelijke informatie wordt aan het bestuur van SGR en aan de Manager Informatieveiligheid verstrekt ten behoeve van de leden van de Datalekkencommissie (zie par. 4.4.) en het datalekkendossier.
- De AP zal na het melden van een datalek een ontvangstbevestiging sturen. Alleen indien de melding daartoe aanleiding geeft zal de AP contact opnemen.
- Bij een datalek als gevolg van een (niet-ethische) hack (art. 138ab van het Wetboek van Strafrecht), wordt onverwijld onderzocht wat de aard van de gelekte persoonsgegevens is, en wat de risico's van misbruik voor de betrokkene(n) zijn. Bij een hack geschiedt naast melding bij de AP, ook aangifte bij de politie in verband met de opsporing van de daders. Aangifte loopt via een eventueel beschikbare contactfunctionaris richting politie.

4.4. Instellen Datalekken Commissie

- De Manager Informatieveiligheid benoemt een Datalekken Commissie bestaande uit ten minste drie leden om verdergaand onderzoek te verrichten. Betrokkenen bij het incident, dan wel het team of de sectie waar het incident heeft plaatsgevonden, kunnen niet participeren in een commissie. Bij de samenstelling van de Datalekken Commissie wordt rekening gehouden met de aard van het incident. De Manager Informatieveiligheid faciliteert waar nodig de Datalekkencommissie.
- De Manager Informatieveiligheid]formuleert in samenspraak met de CG een opdracht voor de Datalekkencommissie en informeert hierover schriftelijk de Datalekkencommissie, voorzien van de termijn waarbinnen het bestuur van SGR de rapportage wil ontvangen en voegt toe Bijlage 3 'Informatie voor leden van de Datalekkencommissie', Bijlage 4 'Informatie voor te interviewen interne personen door de Datalekkencommissie' en Bijlage 5 'Informatie voor te interviewen (medewerkers van) derden door de Datalekken Commissie'.

4.5. Startbijeenkomst Datalekken Commissie

- De Manager Informatieveiligheid plant een startbijeenkomst ter bespreking van de opdracht aan de Datalekken Commissie. Deze startbijeenkomst vindt in geval van een datalek plaats binnen één week na de melding van het datalek aan de AP.
- De Manager Informatieveiligheid draagt zorg voor openstelling van alle beschikbare informatie inzake het datalek t.b.v. de leden van de Datalekkencommissie.

4.6. Verrichten datalek onderzoek

- De Datalekkencommissie stelt binnen de gestelde termijn en opdrachtverlening een (systematisch) (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek.
- De Datalekkencommissie onderzoekt verder of en zo ja hoe dergelijke incidenten in de toekomst kunnen worden voorkomen.
- De bevoegdheden van de Datalekkencommissie zijn:
  - de mogelijkheid met iedereen te spreken;
  - alle relevante documenten in te zien;
  - toegang te hebben tot alle plaatsen. Dit alles in het kader van wat de commissie nodig acht ten behoeve van een zorgvuldige analyse;
  - in relatie tot de externe bewerker gelden de afspraken zoals vastgelegd in de bewerkersovereenkomst
- De Datalekkencommissie heeft binnen 4 weken na de startbijeenkomst het onderzoek afgerond.
- De Datalekkencommissie kan in overleg met, of op instigatie van het bestuur van SGR besluiten om externe deskundigen te betrekken bij het onderzoek.
- De Datalekkencommissie analyseert alle gegevens conform Bijlage 6 'Format rapportage Datalekkencommissie' en Bijlage 2 Beleidsregels ”Meldplicht datalekken in de Wet bescherming persoonsgegevens” van de AP.
- Vervolgens stuurt de Datalekkencommissie het conceptrapport ter verdere bespreking aan de Manager Informatieveiligheid en aan de CG.
- De Manager Informatieveiligheid plant, voordat de slotbijeenkomst plaatsvindt, een overleg met de leden van de Datalekkencommissie en de CG]ter voorbespreking van het conceptrapport.
- De Datalekkencommissie legt het conceptrapport ter correctie op feitelijke onjuistheden voor aan de interne en externe geïnterviewden.
- De Datalekken Commissie stelt vervolgens het rapport vast.

4.7. Beoordeling of datalek gemeld dient te worden aan betrokkene(n)

- Indien een datalek is gemeld aan de AP dient tevens vast gesteld te worden of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat, dit ter beoordeling van en advisering door de Datalekkencommissie.
- De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen komt tot stand met behulp van de schema’s te vinden in de beleidsregels ”Meldplicht datalekken in de Wet bescherming persoonsgegevens” van de AP (zie Bijlage 2). Bij de beoordeling speelt onder meer een rol:
  - Indien SGR passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven (artikel 34a, lid 6, Wbp). Bij twijfel hierover wordt het datalek gemeld aan de betrokkene(n).
  - Het datalek wordt in ieder geval aan de betrokkene(n) gemeld, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, lid 2, Wbp). Dan wel in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn (bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie).

- De melding aan de betrokkene(n) blijft achterwege, als daarvoor zwaarwegende redenen aanwezig zijn (artikel 43 Wbp). Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit noodzakelijk is met het oog op de belangen die worden genoemd in dit artikel. Op grond van artikel 43, onder e, Wbp wordt van de melding aan de betrokkene afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkene.

4.8.Slotbijeenkomst in geval van een datalek: bespreking rapport en vaststellen verbetermaatregelen

- Het bestuur van SGR plant een slotbijeenkomst ter bespreking van het rapport van de Datalekkencommissie.
- Voor de slotbijeenkomst worden uitgenodigd naast het bestuur van SGR de leden van de Datalekkencommissie, de afdelingsmanagers, de Manager Informatieveiligheid, de CG, de ISO en indien communicatie- en/of juridisch advies is ingewonnen, de betreffende adviseurs. De genodigden ontvangen voorafgaand aan de slotbijeenkomst een afschrift van het concept-rapport van de Datalekkencommissie.
- Het bestuur van SGR bespreekt tijdens de slotbijeenkomst het rapport en de voorgestelde geformuleerde verbetermaatregelen.
- Tijdens de bijeenkomst wordt het standpunt van het bestuur van SGR t.a.v. het rapport van de Datalekkencommissie vastgesteld en worden afspraken over verbetermaatregelen vastgelegd. Tijdens de bijeenkomst wordt vast gesteld of en hoe het datalek aan de betrokkene(n) wordt gemeld.
- Na de bijeenkomst ontvangen de genodigden het definitieve rapport.

4.9. Rapporteren aan de betrokkene(n)

- In opdracht van het bestuur van SGR stelt de Manager Informatieveiligheid (indien communicatie- en/of juridisch advies is ingewonnen, in samenspraak met deze adviseurs) een kennisgeving aan betrokkene(n) op.
- De Manager Informatieveiligheid bepaalt in overleg met de CG wat aan de betrokkene(n) wordt gemeld.
- De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van het informatiepunt binnen SGR waar de betrokkene(n) meer informatie over de inbreuk kan krijgen, en de maatregelen die SGR de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.
- De betrokkene(n) worden individueel geïnformeerd.
- Het datalek moet onverwijld gemeld worden aan de betrokkene(n). Dit houdt in dat SGR na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek zodat SGR de betrokkene(n) op een behoorlijke en zorgvuldige manier kan informeren. Wel dient hierbij rekening gehouden te worden dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen.
- In de melding aan de AP is al aangegeven of SGR het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer SGR dat gaat doen. De termijn die SGR in de melding aan het AP aangeeft, moet SGR ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat SGR dit aan de AP weten door middel van een aanpassing van de melding.

4.10. Implementeren verbetermaatregelen

- De manager in wiens domein de verbetermaatregelen liggen is verantwoordelijk dat de vastgestelde verbetermaatregelen worden geïmplementeerd, ziet toe op de communicatie rondom en de uitvoering van de verbetermaatregelen, zorgt dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering, en rapporteert over de voortgang aan het bestuur van SGR.
- Indien bij een bewerker verbetermaatregelen nodig zijn, is het hoofd bedrijfsbureau verantwoordelijk.
- De Manager Informatieveiligheid bewaakt de voortgang, onder eindverantwoordelijkheid van het bestuur van SGR.

4.11. Sluiten melding en vastlegging

- De Manager Informatieveiligheid informeert het bestuur van SGR, het betrokken management, de direct bij het datalek betrokken medewerkers, de CG en de ISO op het moment dat het datalek definitief afgehandeld is en de melding is gesloten.
- De Datalekkencommissie wordt door het bestuur van SGR ontbonden.
- De leden van de Datalekkencommissie vernietigen de nog in bezit zijnde documentatie.
- Het datalek-dossier wordt digitaal bij de CG en bij de Manager Informatieveiligheid gearchiveerd voor de duur van minimaal 1 jaar. Er kunnen redenen zijn om gedurende langere tijd te archiveren, de richtlijn zoals beschreven in Bijlage 2 “Meldplicht datalekken in de Wet bescherming persoonsgegevens; beleidsregels” zal worden gehanteerd.

Deze Procedure Meldplicht Datalekken is in concept vastgesteld door het bestuur van SGR d.d. 15 juni 2017. Het bestuur heeft de Raad van Toezicht in kennis gesteld van deze procedure.

De MR heeft 19 juli 2017 ingestemd met de ze procedure.

De procedure is binnen SGR bekend gemaakt door publicatie op de website en melding hiervan in het weekbericht.

Bijlage 1 Formulier voor melding datalek

Deze bijlage bevat de gegevens die moeten worden opgegeven als een datalek wordt gemeld aan de AP. Dezelfde gegevens worden gebruikt t.b.v. de melding en afhandeling binnen SGR.

Aard van de melding

1) Is dit een vervolg op een eerdere melding? (Kies een van de volgende opties.)

a) Ja
b) Nee

2) Wat is het nummer van de oorspronkelijke melding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord.)

3) Wat is de strekking van de vervolgmelding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord, kies een van de volgende opties.)

a) Toevoegen of wijzigen van informatie betreffende de eerdere melding
b) Intrekking van de eerdere melding

4) Wat is de reden van intrekking? (Beantwoord deze vraag als u bij vraag 3 gekozen heeft voor optie b.)

Wettelijk kader voor de melding

5) Op grond van welke wettelijke bepaling doet u deze melding?

a) artikel 34a, eerste lid, van de Wet bescherming persoonsgegevens
b) artikel 11.3a, eerste lid, van de Telecommunicatiewet

Algemene informatie en contactgegevens

6) Over welk bedrijf of welke organisatie gaat het? (Vul de onderstaande gegevens in.)

a) Naam van het bedrijf of de organisatie
b) (Bezoek)adres
c) Postcode
d) Plaats

7) Door wie wordt het datalek gemeld? (Vul de onderstaande gegevens in.)

a) Naam van de persoon die meldt

b) Functie van de persoon die meldt
c) E-mailadres van de persoon die meldt
d) Telefoonnummer van de persoon die meldt
e) Alternatief telefoonnummer van de persoon die meldt

8) Met wie kan de AP contact opnemen voor nadere informatie over de melding? (Vul de onderstaande gegevens in indien dit iemand anders is dan de melder van het datalek.)

a) Naam contactpersoon
b) Functie van de contactpersoon
c) E-mailadres van de contactpersoon
d) Telefoonnummer van de contactpersoon
e) Alternatief telefoonnummer van de contactpersoon

9) In welke sector is het bedrijf of de organisatie actief? (Kies een van de onderstaande opties.)

a) ...

Gegevens over het datalek

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

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

a) Minimaal: (vul aan)
b) Maximaal: (vul aan)

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

13) 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

14) Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen.)

a) Lezen (vertrouwelijkheid)
b) Kopiëren
c) Veranderen (integriteit)
d) Verwijderen of vernietigen (beschikbaarheid)
e) Diefstal
f) Nog niet bekend

15) Om welk type persoonsgegevens gaat het? (U kunt meerder 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 leef
i) Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
j) Overige gegevens, namelijk (vul aan)

16) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (U kunt 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

17) 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

18) 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

19) Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen? (Beantwoord deze vraag als u vraag 20 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

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

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

22) 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.)

23) 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 (artikel 43, Wbp), namelijk: (vul aan)
d) Anders, namelijk (artikel 34a, lid 6, Wbp): (vul aan)

Technische beschermingsmaatregelen

24) 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)

25) 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

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

a) Ja
b) Nee
c) Nog niet bekend

27) 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

28) Is naar uw mening deze melding compleet? (Selecteer 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 3 Informatie voor leden van de Datalekken Commissie

Inleiding

Het bestuur van de Openbare Scholengemeenschap Reigersbos (SGR) heeft vastgesteld dat er sprake is van een datalek, dat op grond van de Wet bescherming persoonsgegevens (Wbp) is gemeld aan de Autoriteit Persoonsgegevens (AP).

Het bestuur verwacht uiterlijk binnen 6 weken nadat de melding van het datalek is gedaan de rapportage inzake de feitelijke toedracht van het datalek en een voorstel hoe een dergelijk incident in de toekomst te voorkomen.

Om tot een goede rapportage te komen is het noodzakelijk dat een onderzoek door een Datalekken Commissie wordt verricht.

U heeft ingestemd met deelname aan een ad hoc samengestelde Datalekken Commissie. U bent inmiddels uitgenodigd voor een toelichtend gesprek bij de manager informatieveiligheid. Ter voorbereiding op dit gesprek ontvangt u de volgende informatie die voor u relevant is. Vragen kunt u tijdens het gesprek en lopende het onderzoek stellen.

Inzet tijd

Afhankelijk van de complexiteit van het datalek en de ervaring van de commissieleden, zal … tot …. uur per persoon nodig zijn in een periode van vier weken.

Documenten/informatie

U ontvangt hierbij:

- een afschrift van het meldformulier aan de AP;
- een schriftelijke opdracht van de manager informatieveiligheid, voor het doen van een onderzoek, waarin een termijn is gesteld waarbinnen het rapport beschikbaar dient te zijn voor toezending aan de genodigden;
- indien aanwezig, de eigen verslagen van betrokkenen die op verzoek van de betrokken manager zijn opgesteld;
- de Procedure Melding Datalekken SGR incl. bijlagen. Hierin zijn alle processtappen en ieders bevoegdheden en verantwoordelijkheden beschreven.

Bevoegdheden

Als onderzoeker heeft u de bevoegdheid met iedereen te spreken, alle documenten in te zien en heeft u toegang tot alle plaatsen voor zover van belang voor het onderzoek. Mocht het onderzoek daartoe aanleiding geven, dan heeft u, na voorafgaand overleg met het bestuur, de bevoegdheid een extern deskundige te betrekken bij uw onderzoek. De Coördinator Gegevensbescherming (CG) zal u informeren over uw bevoegdheden in relatie tot de bewerker op grond van de bewerkersovereenkomst tussen SGR en de bewerker.

Gesprekken (intern en extern) betrokkenen

Als onderzoekers zult u naast het doen van onderzoek ook gesprekken met (intern) betrokkenen houden, inclusief (indien van toepassing) derde partijen die voor SGR werken.

Ook kan het noodzakelijk zijn om een gesprek te voeren met betrokkene(n) volgens de definitie van Wbp (ofwel de personen om wiens gegevens het gaat) of diens wettelijk vertegenwoordiger(s).

Een methode om in korte tijd de gesprekken met betrokkenen te houden is de zogenaamde 'carrouselmethode'. Dit houdt in dat u achter elkaar de betrokkenen voor een gesprek ontvangt.

Het integraal management of daarmee gelijkgesteld manager van de betrokken afdeling (waar het datalek zich voordeed) zal vergaderruimtes bespreken en afspraken voor gesprekken plannen met betrokkenen. Bij bevestiging van de afspraak dient Bijlage 4 bij de Datalekken procedure meegezonden te worden aan de interne personen die worden geïnterviewd en Bijlage 5 voor de externe personen (medewerkers van derden). Deze bijlage bevat relevante informatie voor de te interviewen personen.

Van belang is een schriftelijk verslag te maken van een gesprek met een (intern of extern) betrokkene, en ter beoordeling op feitelijke onjuistheden toe te zenden aan de betrokkene. Zij ontvangen niet de (concept) rapportage.

U kunt daar waar nodig de ontvangen informatie verwerken in uw rapportage aan het bestuur.

(Eind)rapportage Datalekken Commissie

Bijlage 6, format rapportage Datalekken Commissie, dient als handvat tijdens het uitvoeren van het onderzoek en is voor u leidend bij het opstellen van uw rapportage aan het Bestuur.

Vervolgens wordt de conceptrapportage doorgestuurd naar de [manager informatieveiligheid die tezamen met de CG met uw commissie het conceptrapport bespreekt. U ontvangt daartoe een uitnodiging van de manager informatieveiligheid.

Uw definitieve rapport dient u toe te zenden aan de manager informatieveiligheid binnen de in de opdrachtformulering gestelde termijn.

Uw definitieve rapportage wordt vervolgens besproken met het bestuur, de betreffende afdelingsleider of daarmee gelijkgesteld manager, de leden van de Datalekken Commissie, de manager informatieveiligheid, de CG, de Information Security Officer, en wanneer dat nodig is een communicatie adviseur en een juridisch adviseur.

Het bestuur besluit of de uitkomsten van uw rapport al dan niet worden overgenomen en besluit tevens welke verbetermaatregelen worden doorgevoerd.

Tevens stelt de CG in opdracht van het bestuur een kennisgeving aan betrokkene(n) volgens Wbp op, in overleg met de manager informatieveiligheid eventueel ook in overleg met een communicatie adviseur en een juridisch adviseur.

Als lid van de Datalekken Commissie dient u daarna alle papieren en digitale documenten verband houdende met het datalek te vernietigen. Het datalekken dossier wordt gedurende minimaal één jaar digitaal bij de CG en de manager informatieveiligheid gearchiveerd.

Evalueren eindrapportage en procesgang Datalekken onderzoek

De manager informatieveiligheid evalueert de procesgang van het onderzoek en de eindrapportage met de Datalekken Commissie.

Aanspreekpunten

De betrokken afdelingsleider of daarmee gelijkgesteld manager is aanspreekpunt wat betreft inhoudelijke zaken rondom het datalek en afstemming naar de betrokken afdeling/het betrokken team/de betrokken sectie.

De manager informatieveiligheid coördineert intern het Datalekken onderzoek. Deze manager is beschikbaar in geval u bijvoorbeeld vragen heeft of overleg wilt over de gegeven opdracht, de (concept)rapportage, gestelde termijnen en/of de werkwijze van de AP.

Met vriendelijke groet,

H. Beerepoot,

Manager informatieveiligheid

Bijlage 4 Informatie voor de te interviewen interne personen door de Datalekken Commissie. (Aparte e-mail maken met bevestiging afspraak, wanneer, waar, met wie, hoeveel tijdsbeslag, met deze brief als bijlage.)

Beste collega,

U bent gevraagd mee te werken aan een incidentonderzoek. Hieronder geven wij u informatie over de aanleiding van ons verzoek, de wijze waarop het onderzoek wordt uitgevoerd, uw rol en positie in het onderzoek en het verdere verloop van de procedure.

Aanleiding van ons verzoek

Op grond van de Wet bescherming persoonsgegevens is het bestuur van de Openbare Scholengemeenschap Reigersbos (SR) gehouden om datalekken te melden aan de Autoriteit Persoonsgegevens (AP). Gemeld moet worden ieder datalek waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Binnen onze organisatie is daartoe vastgesteld de procedure 'Melding Datalekken' (bijlage). Recent heeft zich een gebeurtenis binnen onze organisatie voorgedaan, die door het bestuur als datalek is gemeld aan de AP. Op grond van deze procedure heeft de manager informatieveiligheid een Datalekken Commissie ingesteld, die bestaat uit de volgende personen: _____ (invullen personen). Deze commissie verricht onderzoek naar de feitelijke toedracht van het incident en adviseert over eventueel te nemen maatregelen ter voorkoming van het incident in de toekomst. Deze commissie heeft, om haar werk goed te kunnen uitvoeren, de bevoegdheid gekregen om met iedereen te spreken, alle documenten in te zien, en heeft ook toegang tot alle plaatsen. De Datalekken Commissie analyseert alle gegevens en stelt daarna een in beginsel geanonimiseerd intern rapport op aan het bestuur.

Wat betekent dat voor u?

Om een datalek goed te kunnen analyseren wordt tijdens het onderzoek zoveel als mogelijk gebruik gemaakt van de kennis van betrokken medewerkers en deskundigen op het gebied waarop een incident zich afspeelde.

De Datalekken Commissie heeft daarom een afspraak met u gemaakt. Het doel is van u te leren wat er is gebeurd en welke maatregelen genomen kunnen worden om herhaling van vergelijkbare incidenten te voorkomen.

Wat gebeurt er met de informatie die u geeft?

Openheid is essentieel in een dergelijk onderzoek. Alleen bij volledige openheid kunnen de echte oorzaken van incidenten worden achterhaald en beoordeeld.

De Datalekken Commissie maakt een schriftelijk verslag van het gesprek met u, en dit wordt ter beoordeling op feitelijke onjuistheden aan u toe gezonden.

De informatie die u geeft, kan gebruikt worden voor het rapport van de Datalekken Commissie aan het bestuur. Het integrale rapport wordt niet aan u verstrekt.

Het doel van het rapport is inzicht te geven in het incident en om aanbevelingen te doen voor maatregelen om herhaling te voorkomen. Het rapport is vertrouwelijk en in beginsel volledig anoniem. Het rapport wordt aangeboden aan het bestuur, waarna het rapport wordt besproken. Vervolgens besluit het bestuur of hij kan instemmen met de uitkomsten van het rapport en welke verbetermaatregelen genomen dienen te worden. De betreffende afdelingsleider of daarmee gelijkgesteld manager is verantwoordelijk voor de uitvoering van de maatregelen.

Wie ontvangt een afschrift van het rapport?

In de procedure Melding Datalekken staat beschreven wie een afschrift ontvangt van de rapportage.

De informatie uit de rapportage is vaak abstract en organisatie overstijgend. Het is noodzakelijk dat het integraal management of de daarmee gelijkgesteld manager zorgen voor een vertaling naar de afdeling en uitleg geven.

Stilgestaan wordt bij de ervaringen van intern betrokkenen en wat op de afdeling beter of anders kan naar aanleiding van het datalek.

Kan ik vrijuit praten of kan ik hier later nog problemen mee krijgen?

Het is wenselijk dat u de Datalekken Commissie alle benodigde informatie verstrekt om een goede analyse te kunnen maken van het gebeuren en passende verbetermaatregelen te kunnen nemen. Er zullen uitsluitend sanctiemogelijkheden bv in arbeidsrechtelijke zin zijn, indien het geheel van omstandigheden dit rechtvaardigt.

Overige partijen die belang hebben bij de informatie

Ook de betrokkene(n) volgens Wbp (degene op wie een persoonsgegeven betrekking heeft), of diens wettelijk vertegenwoordiger(s) ontvangen informatie van SGR over het datalek, de uitkomsten van het verrichte interne onderzoek, en de eventuele genomen verbetermaatregelen.

Bewaren onderzoeksgegevens/rapportages

Uitsluitend de rapportage aan de AP en het definitieve rapport van de Datalekken Commissie worden gedurende minimaal één jaar digitaal bij de Coördinator Gegevensbescherming gearchiveerd.

Wij danken u bij voorbaat voor het feit dat u uw medewerking wilt verlenen aan het onderzoek.

Met vriendelijke groeten,

De Datalekken Commissie

Bijlage: procedure 'Melding datalekken'

Bijlage 5 Informatie voor de te interviewen (medewerkers van) derden door de Datalekken Commissie.

(Variabele gegevens invullen). Aparte brief maken met bevestiging afspraak, wanneer, waar, met wie, hoeveel tijdsbeslag, met als bijlage deze brief.)

Geachte XXXX (naam invullen),

U is gevraagd mee te werken aan het incidentonderzoek waarbij XXXX (invullen wat van toepassing is) is betrokken. Hieronder geven wij u informatie over de aanleiding van ons verzoek, de methode van onderzoek, uw rol en positie in het onderzoek en het verdere verloop van de procedure.

Aanleiding van ons verzoek

Op grond van de Wet bescherming persoonsgegevens is het bestuur van onze organisatie gehouden om datalekken te melden aan de Autoriteit Persoonsgegevens (AP). Gemeld moet worden ieder datalek waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Recent heeft zich een gebeurtenis voorgedaan waarbij XXXX betrokken is geweest (kort vermelden wie/wat het incident betreft). Dit incident is door het bestuur als datalek gemeld aan de AP. Het bestuur heeft een Datalekken Commissie ingesteld, die bestaat uit de volgende personen: XXXX (leden Datalekken Commissie invullen, naam en functie). Deze commissie verricht onderzoek naar de feitelijke toedracht van het datalek en adviseert over eventueel noodzakelijk te nemen maatregelen ter voorkoming van een dergelijk incident in de toekomst. Deze commissie heeft, om haar werk goed te kunnen uitvoeren, de bevoegdheid gekregen om met iedereen te spreken, alle documenten in te zien, en heeft ook toegang tot alle plaatsen. De Datalekken Commissie analyseert alle gegevens en stelt daarna een in beginsel geanonimiseerd intern rapport op aan het bestuur.

Wat betekent dat voor u ?

Om een datalek goed te kunnen analyseren wordt tijdens het onderzoek zoveel als mogelijk gebruik gemaakt van de kennis van betrokkenen bij het incident. De Datalekken Commissie heeft daarom een afspraak met u gemaakt om ook uw ervaringen te horen. Het doel is van u te vernemen wat er is gebeurd en welke maatregelen genomen kunnen worden om herhaling van vergelijkbare incidenten te voorkomen.

Wat gebeurt er met de informatie die u geeft ?

Openheid is essentieel in een dergelijk onderzoek. Alleen bij volledige openheid kunnen de echte oorzaken van incidenten worden achterhaald en beoordeeld.

De Datalekken Commissie maakt een schriftelijk verslag van het gesprek met u, en dit wordt ter beoordeling op feitelijke onjuistheden aan u toe gezonden.

De informatie die u geeft, kan gebruikt worden voor het rapport van de Datalekken Commissie aan het bestuur.

Het doel van het rapport is inzicht te geven in het incident en om aanbevelingen te doen voor maatregelen om herhaling te voorkomen. Het rapport betreft een intern rapport, is vertrouwelijk en in beginsel volledig anoniem.

Het rapport wordt aangeboden aan het bestuur, waarna het rapport wordt besproken. Vervolgens besluit het bestuur of hij kan instemmen met de uitkomsten van het rapport en welke verbetermaatregelen genomen dienen te worden.

Het bestuur zal de uitkomsten van het rapport en de te nemen verbetermaatregelen op passende wijze bespreken met de bewerker/ de verantwoordelijke leidinggevende van uw bedrijf.

Mocht u nog vragen hebben dan kunt u deze tijdens het gesprek stellen aan de leden van de Datalekken Commissie.
Wij danken u bij voorbaat voor het feit dat u uw medewerking wilt verlenen.

Met vriendelijke groeten,

De Datalekken Commissie

Bijlage 6 Format rapportage Datalekken Commissie

Datalekken rapportage

<Organisatieonderdeel invullen>

Openbare Scholengemeenschap Reigersbos

Datum concept: <invullen>

Datum bespreking CvB: <invullen>

Datum definitief: <invullen>

Datalekken Commissie:

- <naam invullen>
- <naam invullen>
- <naam invullen>

Inhoudsopgave

Gebruikte afkortingen

1. Opdracht en taakstelling

1.1 Datum incident

1.2 Samenstelling Datalekken Commissie

De samenstelling van de Datalekken Commissie is als volgt:

De leden van de Datalekken Commissie hebben het onderzoek volledig onafhankelijk kunnen uitvoeren en zijn niet betrokken geweest bij de behandeling van de betreffende patiënt.

1.3 Volledige beschrijving van incident

1.4 Opdracht aan Datalekken Commissie

2. Algemene informatie

2.1 Persoonsgegevens

2.2 Aard van inbreuk

2.3 Gevolgen voor de betrokkene(n)

2.4 Informeren betrokkene(n)

2.5 Volledig overzicht intern en extern betrokken medewerkers

Naam	**Functie**

2.6 Interviews met intern en extern betrokken medewerkers

Voor dit datalekken onderzoek zijn de volgende interviews gehouden:

3. Het onderzoek

3.1 Focus onderzoek

4. Basisoorzaken incident

4.1 Oorzaken

4.2 Bespreking oorzaak-en-gevolg factoren en veiligheidsbarrières

4.3 Schade voor de betrokkene(n)

4.4 Nevenbevindingen

4.5 Vermijdbaarheid

5. Professionaliteit

5.1 Professionele standaarden en protocollen

5.2 Andere bevindingen rondom professionaliteit

6. Organisatorische aspecten

6.1 Bevindingen rondom organisatorische aspecten

6.2 Bevindingen rondom technische aspecten

7. Conclusie

8. Adviezen en verbetermaatregelen

Verbetermaatregel	Verantwoordelijke	Termijn afgerond

9. Bronnen

Bijlagen