PrimAH

Stichting PrimAH

Procedure
Melden beveiligingsincidenten

Openbaar Primair Onderwijs Aa en Hunze

www.primah.org

Inhoud

Inleiding

Deze procedure voorziet in een gestructureerde wijze voor het melden van datalekken in het kader van de AVG. Daarnaast is er een schema opgenomen om te beoordelen of een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens dan wel aan de betrokkene.

Begrippen

Persoonsgegeven

Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

Verantwoordelijke

De natuurlijke persoon, rechtspersoon of ieder ander die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt;

Bewerker

Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

Verwerking

Elke handeling(en) m.b.t. persoonsgegevens, waaronder verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiding, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen of vernietigen van gegevens.

Bijzondere persoonsgegevens:

- ✓ Godsdienst of levensovertuiging
- ✓ Ras
- ✓ Sexuele leven
- ✓ Poltitieke gezindheid
- ✓ Lidmaatschap vakvereniging
- ✓ Gezondheid (medische gegevens)
- ✓ Strafrechtelijke gegevens

MIBP

De interne aangewezen Manager Informatiebeveiliging en Privacy (MIBP).

Reikwijdte van de meldplicht datalekken

Indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens als bedoeld in artikel 13 van Wbp die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens dan wordt dit als een datalek gekwalificeerd en zal dit bij de Autoriteit Personengegevens (voormalig CBP) moeten worden gemeld. Er moet dus sprake zijn van het 'lekken van data' en dat het lekken een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg heeft. Een enkele tekortkoming of kwetsbaarheid in de beveiliging is geen datalek. Dit is wel het geval wanneer redelijkerwijs niet kan worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid.

Datalekken kunnen ontstaan door:

- ✓ moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware besmetting);
- ✓ technisch falen (ICT-storingen);
- ✓ menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen/meekijken bij intypen wachtwoord);
- ✓ calamiteit (brand datacentrum, wateroverlast);
- ✓ verloren USB stick, laptop, tablet, smartphone;

- ✓ zonder toezicht afdrukken uit de printer;
- ✓ verzenden van email aan verkeerde geadresseerde of met emailadressen van alle geadresseerden;
- ✓ maar ook de onrechtmatige verwerking van gegevens door derden (geen bewerkersovereenkomst)

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens, is verplicht dit direct te melden aan de MIBP via privacy@primah.org .

2. De MIBP is verantwoordelijk voor het onderzoeken van het incident.

3. De MIBP informeert het bestuur over het incident en de ernst van de situatie.

3. De MIBP is verantwoordelijk voor de beoordeling van het datalek en bij een meldplichtig datalek voor het doen, aanvullen en intrekken van de meldingen van datalekken bij de Autoriteit Persoonsgegevens.

4. Het coördinator van het PrimAH ICT Team (PIT) is verantwoordelijk voor het ondernemen van preventieve en repressieve acties, daarbij worden de aanwijzingen van de MIBP in acht genomen.

5. Het bestuur van Stichting PrimAH is verantwoordelijk voor de actualiteit en naleving van deze procedure.

Uitvoering

1. De medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens meldt dit direct aan de MIBP via privacy@primah.org onder vermelding van het onderwerp "datalek".

2. de MIBP onderzoekt het incident. Hierbij is aandacht voor de volgende aspecten. Handvat bij deze beoordeling vormt bijlage 1:

   a. wat is de aard van het datalek?
   b. wat is de oorzaak dat dit incident heeft plaatsgevonden?
   c. is er sprake van het niet nakomen van-, of een tekortkoming in de beveiligingsprocedures?
   d. is de organisatie verwijtbaar?
   e. van het incident wordt een verslag gemaakt en in PrimAHnet vastgelegd, in dit verslag wordt de betreffende melding ook opgenomen.

3. Als er is vastgesteld dat er sprake is van een meldplichtig datalek doet de MIBP binnen 3 werkdagen een melding van het datalek aan de Autoriteit Persoonsgegevens. Teven doet de MIBP verslag aan het bestuur van de melding.

4. De MIBP onderhoudt contact met de Autoriteit Persoonsgegevens over de melding datalekken. Eventuele aanwijzingen van de Autoriteit Persoonsgegevens worden vastgelegd en opgevolgd.

5. Waar nodig en ter beoordeling van het bestuur worden Raad van Toezicht en GMR geïnformeerd over het datalek.

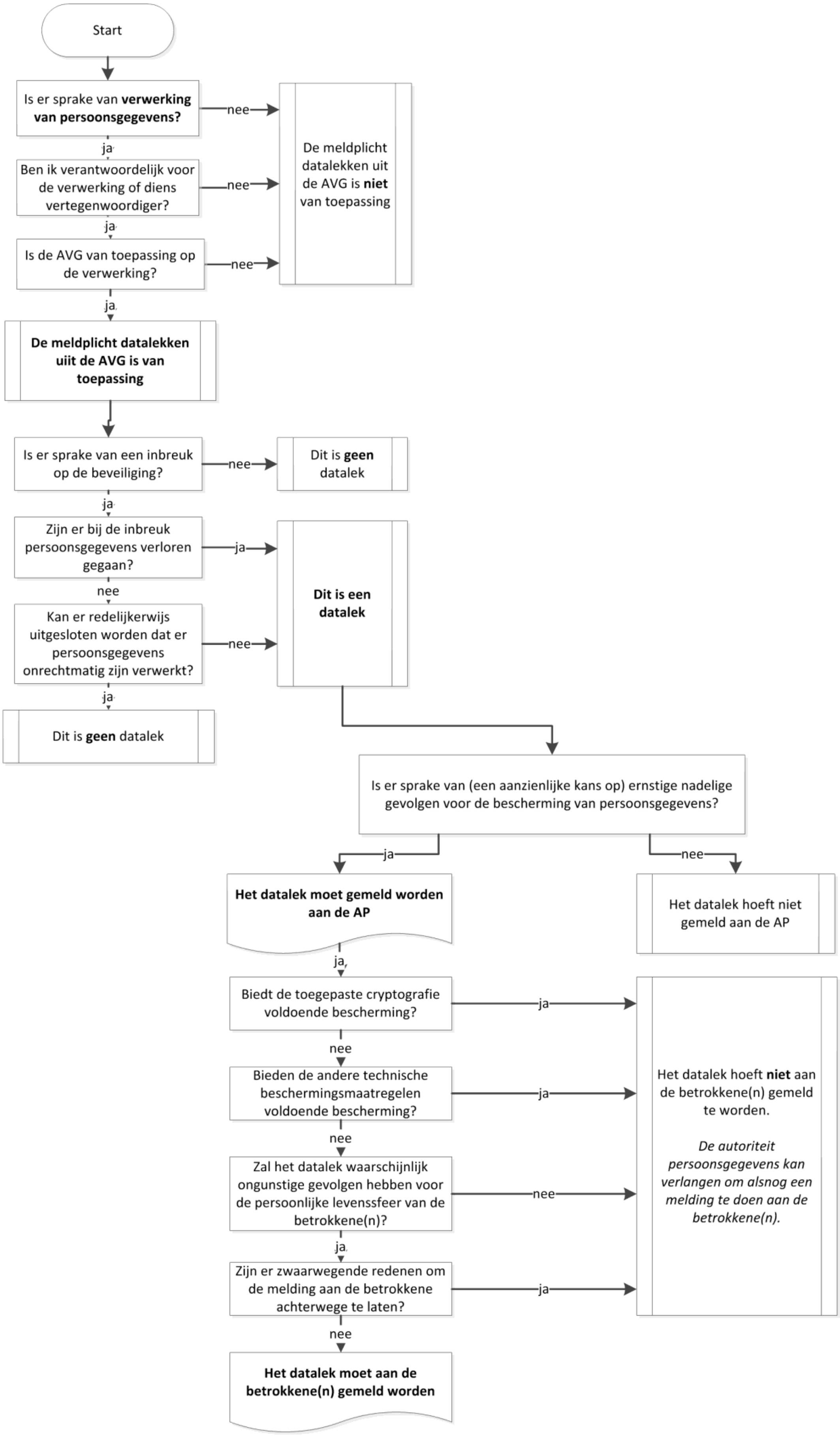
Interne controle

1. Op basis van de gedurende een jaar ontvangen meldingen, analyseert het bevoegd gezag, samen met de MIBP, de meldingen en stellen een verbeterplan op.

2. Minimaal jaarlijks beoordeelt het bevoegd gezag of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

Bijlage 1

Beoordelingsschema datalek


Start
Is er sprake van verwerking van persoonsgegevens?
nee
De meldplicht datalekken uit de AVG is niet van toepassing
ja
Ben ik verantwoordelijk voor de verwerking of diens vertegenwoordiger?
nee
ja
Is de AVG van toepassing op de verwerking?
nee
ja
De meldplicht datalekken uiit de AVG is van toepassing
Is er sprake van een inbreuk op de beveiliging?
nee
Dit is geen datalek
ja
Zijn er bij de inbreuk persoonsgegevens verloren gegaan?
ja
Dit is een datalek
nee
Kan er redelijkerwijs uitgesloten worden dat er persoonsgegevens onrechtmatig zijn verwerkt?
nee
ja
Dit is geen datalek
Is er sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens?
ja
nee
Het datalek moet gemeld worden aan de AP
Het datalek hoeft niet gemeld aan de AP
ja
Biedt de toegepaste cryptografie voldoende bescherming?
ja
Het datalek hoeft niet aan de betrokkene(n) gemeld te worden.
De autoriteit persoonsgegevens kan verlangen om alsnog een melding te doen aan de betrokkene(n).
nee
Bieden de andere technische beschermingsmaatregelen voldoende bescherming?
ja
nee
Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene(n)?
nee
ja
Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten?
ja
nee
Het datalek moet aan de betrokkene(n) gemeld worden

Bijlage 2

Invulformulier Datalek

Invulformulier datalek

Deze bijlage bevat de gegevens die u op moet geven als u een datalek meldt aan de Autoriteit Persoonsgegevens. Bij het formulier zijn de vragen uit bijlage I bij de Europese Verordening 611/2013 als uitgangspunt gehanteerd.

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.)

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

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

Naam van het bedrijf of de organisatie

Bezoekadres

Postcode

Plaats

KvK-nummer

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

Naam van de persoon die meldt

Functie van de persoon die meldt

E-mailadres van de persoon die meldt

Telefoonnummer van de persoon die meldt

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

Naam contactpersoon

Functie van de contactpersoon

E-mailadres van de contactpersoon

Telefoonnummer van de contactpersoon

9. In welke sector is het bedrijf of de organisatie actief?

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 leeftijd

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)

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

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 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

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. 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.)

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, namelijk: (vul aan)

d. Anders, namelijk: (vul aan)

24. Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?[57] (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.)

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

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