Regeling datalekken StOVOG

Algemeen

Deze regeling voorziet in een gestructureerde wijze voor het melden van datalekken in het kader van de Wbp. Daarnaast is er een schema opgenomen om te beoordelen of een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens dan wel aan de betrokkene. Deze regeling is vastgesteld door het College van Bestuur van de Stichting Openbaar Voortgezet Onderwijs Gouda per 2 september 2016 en zal gepubliceerd worden op de website van de stichting.

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 directie van de instelling.
2. De directie van de instelling en de systeembeheerder zijn verantwoordelijk voor het onderzoeken van het incident.
3. De directie van de instelling is verantwoordelijk voor de beoordeling van het datalek en bij een meldplichtige datalek voor het doen, aanvullen en intrekken van de meldingen van datalekken bij de Autoriteit Persoonsgegevens.
4. De systeembeheerder is verantwoordelijk voor het ondernemen van preventieve en repressieve acties, daarbij worden de aanwijzingen van de directie van de instelling in acht genomen.
5. Het College van Bestuur is samen met de directie van de instelling verantwoordelijk voor de actualiteit van deze procedure.

Uitvoering

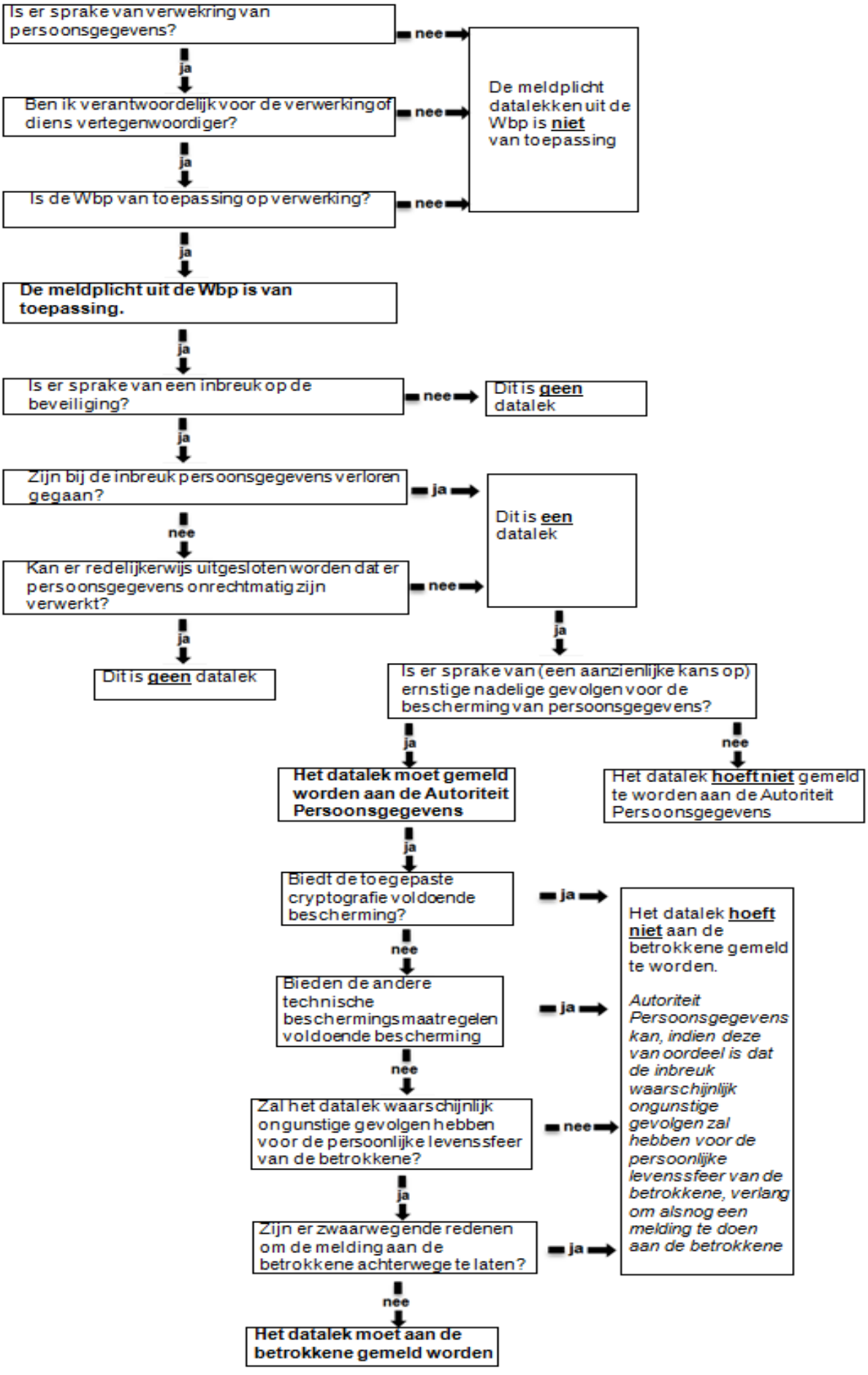
1. De medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens meldt dit direct aan de directie en de systeembeheerder. De melding wordt gedaan via e-mail, onder vermelding ‘datalekken’.
2. De directie, in samenwerking met de systeembeheerder, onderzoekt de melding. Hierbij is aandacht voor de volgende aspecten:
   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 vastgelegd.
3. Als er is vastgesteld dat er sprake is van een meldplichtige datalek doet de directie een melding van het datalek aan de Autoriteit Persoonsgegevens.
4. De directie onderhoudt contact met de Autoriteit Persoonsgegevens over de melding datalekken. Eventuele aanwijzingen van de Autoriteit Persoonsgegevens worden vastgelegd en opgevolgd.

Interne controle

1. Op basis van de, gedurende een jaar, ontvangen meldingen analyseert het College van Bestuur, samen met de directie en met de systeembeheerder, deze en stellen een verbeterplan of -advies op. Dit plan of advies wordt opgenomen in de jaarlijks uit te brengen managementrapportage;
2. Minimaal jaarlijks beoordeelt het College van Bestuur 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.

Schema beoordeling datalek

Onderstaand schema geeft aan hoe een datalek wordt beoordeeld en of deze gemeld moet worden aan de Autoriteit Persoonsgegevens en/of de betrokkene. De stappen in het schema worden altijd doorlopen. Hiervan wordt een verslag gemaakt.


Is er sprake van verwekring van persoonsgegevens?
nee
De meldplicht datalekken uit de Wbp is niet van toepassing
ja
Ben ik verantwoordelijk voor de verwerking of diens vertegenwoordiger?
nee
ja
Is de Wbp van toepassing op verwerking?
nee
ja
De meldplicht uit de Wbp is van toepassing.
ja
Is er sprake van een inbreuk op de beveiliging?
nee
Dit is geen datalek
ja
Zijn 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
ja
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 Autoriteit Persoonsgegevens
Het datalek hoeft niet gemeld te worden aan de Autoriteit Persoonsgegevens
ja
Biedt de toegepaste cryptografie voldoende bescherming?
ja
Het datalek hoeft niet aan de betrokkene gemeld te worden.
Autoriteit Persoonsgegevens kan, indien deze van oordeel is dat de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, verlang om alsnog een melding te doen aan de betrokkene
nee
Bieden de andere technische beschermingsmaatregelen voldoende bescherming
ja
nee
Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene?
nee
ja
Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten?
ja
nee
Het datalek moet aan de betrokkene gemeld worden

Bijlage: 'Gegevens in de melding[1]

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.

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
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

1. 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 contactgevens

1. Over welk bedrijf of welke organisatie gaat het? (Vul de onderstaande gegevens in.)
    a) Naam van het bedrijf of de organisatie
    b) Bezoekadres
    c) Postcode
    d) Plaats
    e) KvK-nummer

2. 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

3. 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.)
    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

[1] Bijlage Beleidsregels 'De meldplicht datalekken in de Wbp', Autoriteit Persoonsgegevens.

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

Gegevens over het datalek
Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

1. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
    a. Minimaal: (vul aan)
    b. Maximaal: (vul aan)

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

3. 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

4. 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

5. 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)

6. 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)

7. Vervolgacties naar aanleiding van het datalek. 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

1. 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

2. 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

3. Wat is de inhoud van de melding aan de betrokkenen? (letterlijke weergave, beantwoord deze vraag als u vraag 1 van dit onderdeel met ja hebt beantwoord.)

4. Hoe veel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord.)

5. 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 1 met ja hebt beantwoord.)

6. Waarom ziet u af van het melden van het datalek aan de betrokkenen? (Beantwoord deze vraag als u vraag 1 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

1. 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)

2. 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 1 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

1. Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)
    a. Ja
    b. Nee
    c. Nog niet bekend

2. 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

1. 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