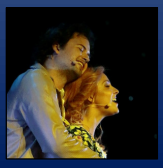
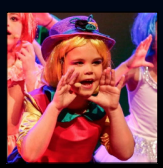
HET BRABANTS MUZIEK-THEATER


- **Stichting Het Brabants Muziek-Theater**
- Mgr. van de Venstraat 39A | 5482 EL |Schijndel
- Tel. (06) 51 500 247
- email: secretariaat@brabantsmuziektheater.nl
- Internet: www.brabantsmuziektheater.nl
- Bankrekening: NL25 RABO 0327 2335 67
- Kamer van Koophandel: 41084368
- BTW nummer: NL009789121.B01


HET BRABANTS MUZIEK-THEATER Kleintje BMT




**PROTOCOL DATALEKKEN**



HET BRABANTS MUZIEK-THEATER

# protocol datalekken Stichting Brabants Muziek-Theater

**betreffende procedures inzake de melding en afhandeling van datalekken**

**STAPPENPLAN DATALEKKEN**

| **Processtappen** | **Activiteit** | **Verantwoordelijke persoon** |
|---|---|---|
| 1. Er wordt een (mogelijk) datalek ontdekt | - Maak direct intern melding van (mogelijke) datalek<br>- Informeer de verantwoordelijke Contactpersoon | Medewerker die het ontdekt |
| 2. Beoordeel het datalek | - Onderzoek het beveiligingsincident<br>- Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden<br>- Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn<br>- Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden | Aangewezen contactpersoon<br>En/of<br>Functionaris gegevensbescherming |
| 3. Bestrijdt het datalek | - Stop het datalek als het nog kan<br>- Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperken<br>- Leg de acties van de genomen maatregelen vast | Aangewezen contactpersoon<br>En/of<br>Functionaris gegevensbescherming. |
| 4.Vaststellen impact datalek | - Onderzoek het datalek en de gevolgen daarvan<br>- Onderzoek de aard van de gegevens die gelekt zijn<br>- Onderzoek de omvang van de gelekte gegevens<br>- Beoordeel welke impact het lek kan hebben op de betrokken personen<br>- Stel vast wat de nadelige gevolgen kunnen zijn | Aangewezen contactpersoon<br>en de<br>Functionaris Gegevensbescherming |

| | | |
|---|---|---|
| 5. Vaststellen Meld en Herstelaanpak | - Bepaal aanpak/informeren AP<br>- Bepaal aanpak/informeren betrokkenen<br>- Bepaal acties voor nazorg betrokkenen<br>- Bepaal acties voor belang van de organisatie<br>- Bepaal acties voor verbetering beveiliging | Aangewezen contactpersoon<br>Functionaris Gegevensbescherming<br>Bestuur |
| 6. Melden AP* | - Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur<br>- Melding via de website van het AP<br>- Van tevoren kan het Meldformulier Datalekken gebruikt worden | Functionaris Gegevensbescherming |
| 7. Melden betrokkenen** | - Melding via bijvoorbeeld brief<br>- Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn.<br>- Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen | Aangewezen contactpersoon<br>Functionaris Gegevensbescherming<br>Bestuur |
| 8. Uitvoeren herstelwerkzaamheden | - Herstel het datalek<br>- Verbeteren van de beveiliging<br>- Lever nazorg aan de betrokkenen | Aangewezen contactpersoon |
| 9. Optimaliseer het beveiligings- en het Datalek proces | - Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken | Aangewezen contactpersoon<br>Functionaris Gegevensbescherming<br>Bestuur |

* Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

** Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

1. Inleiding

1.1. Dit document beschrijft de handelingen te verrichten door Stichting Brabants Muziek Theater bij een datalek zoals gedefinieerd in de Wet Bescherming Persoonsgegevens (hierna te noemen: Wbp).

1.2. Van een datalek is sprake bij een inbreuk op de beveiliging van persoonsgegevens als bedoeld in artikel 13 van de Wbp. De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

1.3. Een datalek dient onverwijld te worden gemeld aan de Autoriteit Persoonsgegevens (hierna te noemen: AP), en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.

1.4. De meldplicht is eveneens van toepassing op Stichting het Brabants Muziek-Theater als het datalek bij een derde is ontstaan, bijvoorbeeld een bewerker van persoonsgegevens van Stichting het Brabants Muziek-Theater (hierna te noemen: Bewerker).

2. Identificatie van een datalek

2.1. De vrijwilliger of deelnemer van Stichting het Brabants Muziek-Theater die een (mogelijk) datalek constateert, meldt dit incident per omgaande bij de Contactpersoon, zijnde dhr. Van Drunen via het e-mail adres: secretariaat@brabantsmuziektheater.nl.

2.2. Een vrijwilliger of deelnemer van stichting het Brabants Muziek-Theater of een Bewerker is te allen tijde bevoegd zelfstandig een melding te doen aan de contactpersoon. De procedure meldplicht datalekken als omschreven in dit protocol wordt dan gestart.

3. Wanneer moet een datalek worden gemeld?

Incidenten moeten worden gemeld wanneer wordt voldaan aan de volgende criteria:

- een incident waarvoor een ‘aanzienlijke kans’ bestaat op ernstige nadelige gevolgen voor de personen van wie de gegevens zijn zoekgeraakt;

- een incident dat ernstige gevolgen kan hebben voor de bescherming van persoonsgegevens (bijvoorbeeld het verliezen van een USB stick met persoonsgegevens) .

4. Is er sprake van een datalek?

4.1. Zodra er bij de contactpersoon een melding wordt gemaakt van een mogelijk datalek, draagt de contactpersoon zo spoedig mogelijk zorg voor het inventariseren en verzamelen van de informatie die benodigd is voor het (eventueel) melden van een datalek aan de AP. Daarbij kan de informatie van het meldloket van de AP als uitgangspunt dienen. De contactpersoon stel zo spoedig mogelijk de functionaris gegevensbescherming (hierna te nomen: FG) in kennis, zijnde mevr. Fleskens.

4.2. Op basis van de verkregen informatie en bij het vermoeden van een datalek wordt door de FG in samenspraak met het bestuur van de stichting beoordeeld of daadwerkelijk sprake is van een datalek.

4.3. Het bestuur beoordeelt voorts of er acuut maatregelen dienen te worden genomen om de schade zoveel mogelijk te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen.

4.4. Wanneer er sprake is van een incident dat gemeld moet worden aan de AP kan gebruik worden gemaakt van meldingsformulieren die zijn te vinden bij het Meldloket van de AP.

4.5. Bij de beoordeling van de vraag of sprake is van een datalek zijn de volgende factoren van belang:

- is er sprake van onrechtmatige verwerking van persoonsgegevens?

hiermee wordt onder andere gedoeld op de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens of een niet toegestane toegang tot verwerkte persoonsgegevens of de niet toegestane verstrekking daarvan;

- is er sprake van verlies van persoonsgegevens?

dit betekent dat stichting het Brabants Muziek-Theater of de Bewerker deze gegevens niet meer heeft, omdat ze zijn vernietigd of op een andere wijze verloren zijn gegaan;

- is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging?

- kan er redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid?

- zijn er persoonsgegevens van gevoelige aard gelekt?

bijzondere persoonsgegevens (artikel 16 Wbp) zijn onder andere (i) gegevens over de financiële of economische situatie van de betrokkene, (ii) gegevens die kunnen leiden tot stigmatisering of

uitsluiting van de betrokkene, (iii) gebruikersnamen, wachtwoorden en andere inloggegevens en (iv) 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?

bij de beoordeling of daarvan sprake is zijn onder andere van belang: (i) de omvang van de verwerking, (ii) de vraag of het om veel persoonsgegevens per persoon gaat en/of om gegevens van grote groepen betrokkenen, (iii) de impact van verlies of onrechtmatige verwerking van persoonsgegevens, (iv) het delen van de persoonsgegevens met derden waardoor de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens ook elders impact kunnen hebben en (v) betrokkenheid van kwetsbare groepen.

4.6. Indien het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. In dat geval is melding aan de AP niet nodig.

4.7. Indien tot de conclusie wordt gekomen dat sprake is van een (mogelijk) datalek, wordt het communicatietraject richting betrokkene(n) en (eventueel) de betreffende Bewerker besproken.

## 5. Melden aan de Autoriteit Persoonsgegevens

5.1. De FG verzorgt de tijdige melding bij de AP volgens het hierboven onder 4.1 genoemde meldingsformulier van de AP. De melding dient op grond van de Wbp onverwijld, zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek te geschieden. Het bestuur wordt tevens op de hoogte gesteld van de melding.

5.2. De FG fungeert als contactpersoon inzake de communicatie met de AP. Afhankelijk van de aard van het datalek of indien blijkt dat het incident geen datalek is dan de melding aan de AP worden aangevuld of ingetrokken.

5.3. De FG danwel de contactpersoon draagt ervoor zorg dat de bij het incident betrokken personen worden geïnformeerd en stelt zo spoedig mogelijk verslag op van over de toedracht van het incident. Deze schriftelijke informatie wordt aan het bestuur verstrekt ten behoeve van het datalekkendossier.

5.4. Na ontvangst van de melding aan de AP zal de AP daarvan een ontvangstbevestiging sturen. De AP neemt alleen contact op indien de AP daartoe aanleiding ziet.

6. Is sprake van een hack?

Bij een datalek als gevolg van een (niet-ethische) hack (artikel 138ab Wetboek van Strafrecht), is het van belang om vast te stellen wat de aard van de gelekte persoonsgegevens is en wat de risico's van misbruik voor de betrokkene(n) zijn. Bij een hack kan het naast het doen van de melding bij de AP ook zinvol zijn om aangifte te doen bij de politie. De FG zal daarvoor in dat geval in overleg met het bestuur zorgdragen.

7. Dient het datalek te worden gemeld aan betrokkene(n)?

7.1. Indien een datalek is gemeld aan de AP dient te worden vastgesteld of het datalek ook moeten worden gemeld aan degenen om wiens persoonsgegevens het gaat. Het bestuur zal dat in overleg met de FG vaststellen.

7.2. De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen kan tot stand komen met behulp van de overzichten in de beleidsregels 'Meldplicht datalekken in de Wet bescherming persoonsgegevens' van de AP zoals hierboven genoemd.

7.3. Bij de afweging of het datalek dient te worden gemeld aan betrokken is onder andere het volgende van belang:

- indien Stichting het Brabants Muziek-Theater 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. Indien daarover wordt getwijfeld dan dient het datalek aan de betrokkene(n) gemeld te worden;

- het datalek moet aan de betrokkene(n) worden gemeld indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer;

Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn, waarbij kan worden gedacht aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie;

7.4. De melding aan de betrokkene(n) mag achterwege blijven als daarvoor zwaarwegende redenen aanwezig zijn. De melding mag alleen achterwege mag blijven als dit noodzakelijk is met het oog op de belangen die worden genoemd in artikel 43 Wbp ((i) de veiligheid van de staat, (ii) de voorkoming, opsporing en vervolging van strafbare feiten, (iii) gewichtige economische en financiële belangen van de staat en andere openbare lichamen, (iv) het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder (ii) en (iii), of (v) de bescherming van de betrokkene of van de rechten en vrijheden van anderen).

8. Handelwijze melding aan betrokkene(n)

8.1. In opdracht van het bestuur van Stichting het Brabants Muziek-Theater stelt de FG of de Contactpersoon een kennisgeving aan betrokkene(n) op. De FG bepaalt wat aan de betrokkene(n) wordt gemeld.

8.2. De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van Stichting het Brabants Muziek-Theater en een contactpersoon waar de betrokkene(n) meer informatie over de inbreuk kan (kunnen) krijgen, en de maatregelen die Stichting het Brabants Muziek-Theater de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.

8.3. Het datalek moet onverwijld gemeld worden aan de betrokkene(n). Dit betekent dat Stichting het Brabants Muziek-Theater na het ontdekken van het datalek enige tijd mag nemen voor nader onderzoek zodat zij de betrokkene op een behoorlijke en zorgvuldige manier kan informeren. Daarbij dient te allen tijde rekening te worden gehouden met het (eventuele) feit dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene(n) daarover wordt geïnformeerd, hoe eerder deze in actie kan komen.

8.4. De betrokkene(n) worden individueel geïnformeerd.

8.5. In de melding aan de AP is aangegeven of het datalek aan betrokkene(n) is gemeld. Indien de aan de AP aangegeven termijn waarbinnen die melding zou worden gedaan aan de betrokkene(n) niet kan worden gehaald dan dient de FG dit aan de AP door te geven door middel van een aanpassing van de eerdere melding.

9. Datalek-onderzoek en vaststellen verbetermaatregelen

9.1. De FG stelt zo spoedig mogelijk na de vaststelling van het incident een (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek en betrekt daarbij de vraag of en hoe dergelijke incidenten in de toekomst kunnen worden voorkomen.

9.2. In overleg met het bestuur van Stichtng het Brabants Muziek-Theater mag de FG daartoe met relevante personen spreken, alle relevante documenten inzien en toegang hebben tot alle plaatsen, voor zover noodzakelijk voor een zorgvuldig onderzoek;

9.3. De FG kan het bestuur van Stichting het Brabants Muziek-Theater voorstellen om waar nodig externe partijen te betrekken indien dat voor een deugdelijk onderzoek noodzakelijk is.

9.4. De FG rapporteert de conclusies van het hiervoor bedoelde onderzoek zo spoedig mogelijk aan het bestuur van Stichting het Brabants Muziek-Theater.

9.5. In overleg waarbij in ieder geval het bestuur van Stichting het Brabants Muziek-Theater en de FG aanwezig zijn zullen de uitkomsten van het hiervoor genoemde onderzoek worden besproken en afspraken worden gemaakt over verbetermaatregelen om herhaling van het incident zoveel mogelijk te voorkomen.

9.6. Het bestuur van Stichting het Brabants Muziek-Theater ziet er op toe dat de vastgestelde verbetermaatregelen worden geïmplementeerd en in de organisatie worden gecommuniceerd.

10. Datalek-dossier

Het datalek-dossier wordt digitaal bij de FG en het secretariaat bewaard voor de duur van minimaal 1 jaar. Er kan een langere termijn van minimaal 3 jaar van toepassing zijn zoals bedoeld in de beleidsregels ‘Meldplicht datalekken in de Wet bescherming persoonsgegevens’ van de AP, pagina 46.

Aldus op 21 november2019 vastgesteld door het bestuur van Stichting het Brabants Muziek-Theater.