




Aan het college van Burgemeester en Wethouders

Behandelvoorstelnr : 719837
Brunssum, 23 maart 2017

T.b.v. **Interne agenda**
d.d. 18 april 2017

Verantw. Portefeuillehouder
C.J.C.P. de Rijck

Ambtelijke routing	d.d.	Akk.	Bestuurlijke routing	Conf. adv.	Bespr.
Financiële toets	11-4-2017		Burgemeester		
Juridische toets (AJZ)			Wethouder Offermans		
Juridische toets (Controlling)			Wethouder Joosten		
Kwaliteitstoets	11-4-2017		Wethouder Heinen		
Hoofd Afdeling	10-4-2017		Wethouder de Rijck		
Directeur Dienst	11-4-2017		Wethouder Janssen		
			Secretaris		

Uiterste datum B&W vergadering: NVT
Motivatie **fatale termijn** aangeven indien van toepassing: NVT

Onderwerp omschrijving:
Meldplicht Datalekken Protocol

Vorstel/beslispunten:
Uw college wordt voorgesteld te besluiten:
Het college wordt geadviseerd om in te stemmen met het voorgestelde 'Meldplicht Datalekken Protocol' om vervolgens te kunnen voldoen aan Wet Meldplicht Datalekken.

Besluit BW:
AKKOORD
Het college wordt geadviseerd om in te stemmen met het voorgestelde 'Meldplicht Datalekken Protocol' om vervolgens te kunnen voldoen aan Wet Meldplicht Datalekken.

Registratienummer: 719837

1. Onderwerp omschrijving:
Meldplicht Datalekken Protocol

2. Voorstel/beslispunten: Uw college wordt voorgesteld te besluiten:
Het college wordt geadviseerd om in te stemmen met het voorgestelde 'Meldplicht Datalekken Protocol' om vervolgens te kunnen voldoen aan Wet Meldplicht Datalekken.

3. Aanleiding

Op 1 januari 2016 is de Wet bescherming persoonsgegevens aan gepast met de Meldplicht Datalekken en vanaf die datum in werking getreden. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) per direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra persoonsgegevens verloren raken als gevolg van een incident (o.a. systeem falen, menselijke falen) waarbij de kans bestaat of heeft op ernstige nadelige gevolgen voor de betrokkene.

4. Probleemstelling

De gemeente heeft op dit moment geen eenduidig protocol voor hoe te handelen bij datalekken. Hierdoor kan de gemeente op dit moment niet voldoen aan de Wet Meldplicht Datalekken. Medio 2016 heeft het college wel de beleidsregels vastgesteld inzake Datalekken. Deze zijn gelijktijdig vastgesteld met het nieuwe informatiebeveiligingsbeleid (642440)

5. Doelen / beoogd resultaat

a. wat willen we bereiken?

De gemeente Brunssum wil aan de Wet bescherming persoonsgegevens voldoen. De introductie van dit protocol gaat gepaard met de doelstelling van de organisatie om haar informatiebeveiliging naar een hoger niveau tillen, zodat we voldoen aan de Baseline Informatiebeveiliging Gemeenten (BIG).

- Hierbij streven wij als organisatie er naar om tijdig en adequaat datalekken af te handelen, en waar nodig extra beveiligingsmaatregelen aan te scherpen t.b.v. informatieveiligheid en privacy
- Periodiek wordt het aantal datalekken geanalyseerd en aangetoond dat de gemeente aan de Wet bescherming persoonsgegevens voldoet. De resultaten van de analyse worden periodiek in de Informatiebeveiligingsforum (IBF) besproken (multidisciplinaire orgaan op tactisch niveau).
- Jaarlijks wordt schriftelijk gerapporteerd aan B&W, tegelijkertijd met de jaarrekeningcontrole als onderdeel van de paragraaf Bedrijfsvoering.

b. wat gaan we ervoor doen?

- Meldplicht datalekken protocol laten vaststellen door B&W
- De informatiebeveiliging functionaris gaat in samenwerking met functionaris gegevensbescherming presentaties geven om meldplicht datalekken protocol onder de aandacht te brengen en meer bewustzijn te creëren binnen de organisatie. Daarnaast informeren wij onze leveranciers over het protocol.
- De informatiebeveiliging functionaris en functionaris gegevensbescherming houden toezicht op de naleving van het protocol.

c. hoe meten we of het beoogde resultaat is bereikt?

- Indicator: Periodiek worden de gemelde datalekken geanalyseerd door informatiebeveiliging functionaris/ functionaris gegevensbescherming op tijdigheid van de afhandeling. Daarnaast wordt er een analyse uitgevoerd op het type incident/datalek en waar nodig worden beheersmaatregelen opgesteld of aangescherpt.
- Bron: Tijdens periodieke bijeenkomst van het IBF worden de datalekken besproken. Daarnaast wordt er jaarlijks schriftelijk gerapporteerd aan B&W.

6. Kaders

a. algemene beleidskaders (landelijk / provinciaal / lokaal)

- Baseline Informatiebeveiliging Gemeenten (BIG)
- Wet Bescherming Persoonsgegevens (Wbp)

- Algemene Verordening Gegevensbescherming (AVG), de vervangde wetgeving van de Wbp per 25 mei 2018.

b. autonoom beleid / taken in medebewind?

c. past het voorstel in de strategische visie?

- **ja**

- toelichting: Het college heeft kennis genomen van het informatiebeveiligingsbeleid editie 2016 (verseon registratiekenmerk 642635). Hierin is besproken dat zodra het informatiebeveiligingsuitvoeringsplan 2016 (waarin informatiebeveiliging risico's, maatregelen, functies en prioriteiten zijn opgenomen) gereed is, beleidsregels meldplicht datalekken, integraal ter definitieve vaststelling worden aangeboden middels een separaat voorstel. Het college heeft hiermee ingestemd.

d. relatie met programmabegroting?

- programma: Informatiebeveiliging is opgenomen in de paragraaf Bedrijfsvoering en vormt derhalve geen onderdeel van een programma

- beleidsveld: Informatiebeveiliging is gekoppeld aan het taakveld Overhead.

7. Argumenten / overwegingen

Zoals aangegeven vormt het vaststellen van het protocol Meldplicht Datalekken een wezenlijk onderdeel van de uitvoering van ons Informatiebeveiligingsplan (683484) Burgers en bedrijven moeten er op kunnen vertrouwen dat de gemeente Brunssum op een verantwoorde manier veilig met haar gegevens om gaat. Door onder andere:

- de BIG als normenkader te hanteren,
- het Informatiebeveiligingsbeleid hierop af te stemmen,
- maatregelen te treffen en deze continue te monitoren en te verbeteren
- het vaststellen van een protocol inzake meldplicht Datalekken

Geeft de gemeente Brunssum invulling aan een betrouwbare, veilige dienstverlening.

Dat een dergelijk protocol noodzakelijk is blijkt uit het feit dat zich tot op heden al 5 datalekken hebben voorgedaan. Deze waren echter van de categorie 0 waarbij melding aan de autoriteit persoonsgegevens niet noodzakelijk was.

8. Advies

Het college wordt geadviseerd om in te stemmen met het voorgestelde 'Meldplicht Datalekken Protocol' om vervolgens te kunnen voldoen aan Wet Meldplicht Datalekken.

9. Aanpak / uitvoering

a. financiële gevolgen en dekking

Er zijn geen additionele kosten gekoppeld aan de invoering van dit protocol. Mochten er datalekken geconstateerd worden die maatregelen vergen die niet binnen de reguliere budgetten opgepakt kunnen worden dan zal het college hierover een separaat voorstel ontvangen.

- kosten: € (incidenteel / structureel)

- dekking (product- / activiteitencode):

- restantbudget na aftrek kosten: €

- restantbudget voldoende om resterende verplichtingen te dekken: ja / nee

b. risico's?

- omschrijving risico ('s): financieel / anders t.w.: Het niet voldoen aan de Wet Meldplicht Datalekken kan leiden tot boetes van max. 820.000 euro. In de risico-paragraaf is het onderdeel datalekken opgenomen voor het genoemde bedrag..

- omschrijving beheermaatregelen: Inrichten van een Meldplicht Datalekken Protocol zoals voorgesteld.

- gevolgen voor weerstandsvermogen: Nader te bepalen.

c. tijdpad / mijlpalen / vervolgtraject / evaluatie

Vanaf februari zijn diverse presentaties verzorgd rondom datalekken aan de diverse afdelingen om zodoende meer bewustzijn te creëren bij de medewerkers. Na instemming van IB forum per 16-1-2017 is het protocol effectief. Handhaving vindt plaats na akkoord van het college.

d. uitvoerende partners intern en extern (werkstructuur)

Het informatiebeveiligingsforum (IB) onder voorzitterschap van de functionaris Informatiebeveiliging komt periodiek (6 weken) bij elkaar. Het forum kent een zodanige samenstelling dat integraliteit gegarandeerd is met een geborgde koppeling naar het DT. Momenteel nemen de volgende functionarissen deel aan het IB:

- Tijdelijke inhuur CISO (Functionaris Informatiebeveiliging) tevens voorzitter.
- Functionaris Gegevensbescherming, vervangend voorzitter
- Hoofd Informatiemanagement, plaatsvervanger functionaris Informatiebeveiliging
- Directeur
- Hoofd Publieksdiensten
- Hoofd Bestuurszaken
- Consulents P&O

- Coördinator Informatiemanagement.

Het forum ziet toe op een correcte uitvoering van het beleid en het plan, stelt zaken bij en ziet toe op de uitvoering van maatregelen bij datalekken en beveiligingsincidenten.

Daarnaast worden zaken formeel en informeel afgestemd met Parkstad-IT. Dit gebeurt veelal door de contractmanager (hoofd Informatiemanagement).

e. communicatie intern en extern?

- advies / instemming / informatie OR: ja (wat / waarom?) / nee (waarom niet?)
- persbericht: **Nee er is geen persbericht noodzakelijk.** Meldplicht Datalekken Protocol is gericht op onze interne medewerkers en leveranciers. Dit wordt beschouwd als reguliere bedrijfsvoering.
- terinzagelegging: **Nee**
- overig extern: **n.v.t.**

10. Bijlagen

Meldplicht Datalekken Protocol (719952)