Nota voor burgemeester en wethouders
Onderwerp
Gewijzigde procedure datalekken

Team
DEV-CS

1- Notagegevens	
Notanummer	2019-000245
Datum	30-01-2019
Programma:	
01 Burger en bestuur	
Portefeuillehouder Burgemeester	

2- Bestuursorgaan	
[X]B & W	12-02-2019
[ ]Raad	--
[ ]Burgemeester	--

College van B & W	
- Burgemeester	- Weth. Kolkman
- Weth. Grijsen	- Weth. Rorink
- Weth. Verhaar	- Weth. Walder

Besluitenlijst	d.d.		d.d.		d.d.
[ ]Akkoordstukken	--	[X]Openbaar	12-02-2019	[ ]Besloten	--

Routing	d.d.
Burgemeester	07-02-2019
Directeur	06-02-2019
Programmamanager	06-02-2019

	par.
[ ]adj.secr.	--
[X]gem.secr.	07-02-2019
BIS Openbaar	
Status	Definitief2019-02-13

Bijlagen

B & W d.d.: 12-02-2019

Besloten wordt:
1 De Algemeen Directeur te machtigen inbreuken in verband met persoonsgegevens te melden bij de Autoriteit Persoonsgegevens ter voldoening aan het bepaalde in artikel 33 van de Algemene verordening gegevensbescherming met de mogelijkheid ter zake van deze bevoegdheid machtiging te verlenen aan de Privacy Officer;
2 de nota en het besluit openbaar te maken.

Financiële aspecten:

Financiële gevolgen voor de gemeente?	Nee
Begrotingswijziging	Nee

Voorstel openbaarmaking conform Wet Openbaarheid Bestuur (Wob)

[X] De nota en het besluit openbaar te maken
[ ] De nota en het besluit openbaar te maken vergezeld van bijgaand persbericht
[ ] De nota en het besluit openbaar te maken nadat

[ ] De nota en het besluit openbaar te maken, behalve…

[ ] Het besluit openbaar te maken, maar niet de nota, gelet op artikel:

[ ] De nota en het besluit niet openbaar te maken, gelet op artikel:

Kennisgeving/ Bekendmaking Awb

Kennisgeving (publicatie) conform Awb	Nee
Bekendmaking conform Awb	Nee

gemeente Deventer

ADVIESRADEN:

Moet een van de adviesraden gehoord worden of op de hoogte gesteld? Nee

Toelichting

Inleiding

Sinds 1 januari 2016 geldt de meldplicht datalekken. Een datalek is een incident waarbij persoonsgegevens verloren zijn gegaan, waarbij onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden, of wanneer dit niet met zekerheid uitgesloten kan worden. De gemeente Deventer moet datalekken met nadelige gevolgen voor burgers direct melden bij de Autoriteit Persoonsgegevens (AP), de toezichthouder. Op straffe van een geldboete moet dit ieder geval binnen 72 uur gebeuren.

De procedure meldplicht datalekken beschrijft de procedure die gevolgd dient te worden in het geval van een ernstig datalek. Sinds het invoeren van de huidige procedure meldplicht datalekken in 2017 heeft de praktijk geleerd dat deze procedure te weinig houvast biedt. In deze procedure is onvoldoende specifiek beschreven wie welke handelingen verricht bij het volgen van deze procedure. Tevens komt uit deze procedure onvoldoende duidelijk naar voren dat alle drie de DOWR-gemeentes individueel verantwoordelijk zijn voor het melden van een datalek bij de AP.

Het voorstel is dan ook om een gewijzigde procedure meldplicht datalekken door het college te laten vaststellen. De gewijzigde procedure beschrijft uitgebreider de te nemen stappen voor- en na het melden van een datalek door de verschillende actoren. Tevens geeft de procedure aan dat de hierin opgenomen processtappen bij alle drie de gemeentes op gelijke wijze worden ingevuld. Ook wordt specifieker aangegeven hoe de Privacy Officers (de privacyadviseurs) van de verschillende DOWR-gemeentes afzonderlijk incidenten dienen te melden en vast te leggen. Om dit alles kracht bij te zetten is tot slot bij de procedure een zogenaamde rasci-matrix toegevoegd. Deze matrix geeft nog eens helder de rollen en verantwoordelijkheden weer van de personen die bij de procedure meldplicht datalekken betrokken zijn.

Beoogd resultaat

Adequaat optreden bij incidenten ter bescherming van de persoonsgegevens van burgers.

Updaten huidige procedure datalekken.

Verduidelijken verdeling van verantwoordelijkheden m.b.t. het melden van dergelijke incidenten.

Kader

Algemene verordening gegevensbescherming (AVG)

Argumenten voor en tegen

Voor

Procedure die beter aansluit bij de praktijk en de individuele verantwoordelijkheden van de drie DOWR-gemeentes onder de AVG.

Extern draagvlak (partners)

Nvt

Financiële consequenties

Nvt

Aanpak/uitvoering

Het melden van een datalek is geen besluit. Er moet daarom een machtiging via de lijn van de Algemeen

Directeur richting de Privacy officer verstrekt worden.

Het creëren van bewustzijn en het bevorderen van kennis van medewerkers over de procedure bij datalekken bevordert de effectiviteit van deze procedure. Met behulp van intranet zal het vaststellen van de gewijzigde procedure dan ook binnen de organisatie worden gecommuniceerd.

Procedure meldplicht datalekken DOWR

Uitgave : versie 4
Naam : L.M. Schieving
Mail : l.schieving@deventer.nl

Inleiding

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties, zoals gemeentes, die met een ernstig datalek te maken krijgen, dit direct moeten melden bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens (AP) ziet als toezichthouder namelijk toe op de naleving van de Algemene verordening gegevensbescherming (AVG), waarin de belangrijkste regels met betrekking tot de omgang met persoonsgegevens zijn vastgelegd. Persoonsgegevens zijn alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit zijn dus niet alleen naam, adres of burgerservicenummer, maar bijvoorbeeld ook e-mailadressen, (pas)foto's en IP-adressen. In sommige gevallen moeten organisaties bij een ernstig datalek tevens een melding doen bij de mensen van wie de persoonsgegevens zijn gelekt.

Als zich een incident heeft voorgedaan waarbij persoonsgegevens verloren zijn gegaan of wanneer onrechtmatige verwerking van die gegevens heeft plaatsgevonden, of wanneer dit niet met zekerheid uitgesloten kan worden, dan spreken we over een datalek. Dit kan veroorzaakt worden door iets van buitenaf, bijvoorbeeld een hacker die de organisatie binnendringt, maar ook bijvoorbeeld door een medewerker die een laptop met daarop persoonsgegevens in de trein laat liggen. Als een ernstig datalek plaatsvindt, is een gemeente verplicht om hier zonder onnodige vertraging, en binnen 72 uur, een melding van te maken bij de Autoriteit Persoonsgegevens. De ernst van een datalek is afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. Als het lek nadelige gevolgen kan hebben voor de betrokkenen waarvan persoonsgegevens gelekt zijn, moet een organisatie ook deze betrokkenen informeren. Een datalek kan vervelende situaties opleveren voor zowel de organisatie als voor de betrokkenen. Een organisatie loopt bijvoorbeeld het risico op reputatieschade en op financiële gevolgen, terwijl betrokkenen risico lopen op identiteitsfraude of discriminatie. Vanaf 25 mei 2018 kan de Autoriteit Persoonsgegevens, in geval van een ernstig datalek, organisaties boetes opleggen van maximaal 20 miljoen of 4% van de wereldwijde jaaromzet.

Een gemeente is in veel situaties verantwoordelijk voor de verwerking van (bijzondere) persoonsgegevens, waardoor de meldplicht onder de Algemene verordening gegevensbescherming van toepassing is. Omdat deze wetgeving verlangt dat, wanneer een ernstig datalek geconstateerd is, dit lek zo snel mogelijk, en op correcte wijze, gemeld wordt bij de Autoriteit persoonsgegevens en eventuele betrokkenen is het wenselijk om hier een duidelijke procedure voor te hebben.

Procedure

In dit document wordt de procedure beschreven die gevolgd dient te worden in het geval van een incident dat mogelijk een datalek tot gevolg kan hebben. Deze procedure bestaat uit een aantal te doorlopen processtappen die voor elk incident gelijk zijn. Deze procedure is van toepassing op incidenten die in de gemeente Deventer, de gemeente Olst-Wijhe en de gemeente Raalte plaatsvinden. Gezien de samenwerking tussen deze gemeentes, o.a. op het gebied van bedrijfsvoering (DOWR-samenwerking), kiezen de drie gemeentes om dezelfde procedure te volgen als het gaat om de afhandeling van incidenten.

Meldplicht

Een aantal zaken zijn van belang om deze procedure goed te laten werken. Het is belangrijk dat de medewerkers van de individuele gemeentes voldoende kennis hebben over waar ze incidenten moeten melden en weten welke acties zij bij een incident moeten ondernemen. Elke medewerker dient alert te zijn op bedreigingen met betrekking tot gegevensbescherming. De medewerkers van de DOWR ICT-servicedesk, het aangewezen centrale meldpunt voor incidentmeldingen, zijn bijvoorbeeld getraind in hoe zij met meldingen over incidenten om moeten gaan. De overige medewerkers zijn geïnstrueerd over waar en wanneer zij een melding van een incident moeten doen.

Melding incident

Een melding van een incident komt bij de DOWR ICT-servicedesk terecht doormiddel van het invullen van een meldingsformulier door een medewerker in TOPdesk. Dit formulier is digitaal te vinden onder

de knop ‘meldplicht datalekken’. Een centraal meldingspunt is van belang om het meldingsproces zoveel mogelijk te standaardiseren, om versnippering van geregistreerde meldingen te voorkomen en om een totaaloverzicht te behouden van afgehandelde meldingen. De teammanager van de medewerker die de melding bij de servicedesk zou moeten doen, ziet erop toe dat dit formulier bij een incident ook daadwerkelijk wordt ingevuld. Wanneer er een incident bij de servicedesk wordt gemeld, krijgen de Privacy Officer (PO), de privacyadviseur van de gemeente waar het incident betrekking op heeft, de Information Security Officer (ISO) en de Chief Information Security Officer (CISO) een kopie van deze melding binnen. De medewerker van de DOWR ICT-servicedesk wijst de PO van de gemeente waar het incident betrekking op heeft aan als behandelaar. Dit kan de PO van de gemeente Deventer en/of de gemeente Olst-Wijhe en/of de gemeente Raalte zijn.

Onderzoek en impactanalyse

De PO heeft een coördinerende rol op het moment dat er zich een incident heeft voorgedaan. De desbetreffende PO neemt contact op met de medewerker die de melding heeft gedaan en probeert zoveel mogelijk informatie over het incident van de medewerker te verkrijgen. De PO maakt aan de hand van deze informatie een inschatting over of er daadwerkelijk sprake is van een datalek en of er direct actie zal moeten worden ondernomen.

Wanneer het gaat om een incident, dat is ontstaan door een beveiliginginbreuk, wordt de vraag of er direct actie zal moeten worden ondernomen samen met de Information Security Officer (ISO) beantwoord. Wanneer het tevens een ICT-gerelateerd incident betreft, wordt daarbij ook het Computer Emergency Response Team (CSERT) en de Chief Information Security Officer (CISO) ingeschakeld. Het SCERT is ingesteld om snel en adequaat te kunnen reageren op dit soort incidenten. Het CSERT wordt door de CISO bij elkaar geroepen. Afhandeling van het incident door het CSERT verloopt volgens het incident management proces. De verzoeken die het CSERT uitstuurt richting de gemeentelijke organisatie om inzichtelijk te krijgen wat er precies gebeurt is, en wat kan helpen bij het dichten van het lek, dienen zo spoedig mogelijk door de organisatie opgevolgd te worden. De medewerkers van de desbetreffende gemeente dienen daarom goed op de hoogte te zijn van het belang en de urgentie van de verzoeken vanuit dit team.

Maatregelen

De PO van de betreffende gemeente is verantwoordelijk voor het ontwerpen van maatregelen die de ontstane schade minimaliseren (herstelmaatregelen) en maatregelen teneinde nieuwe vergelijkbare incidenten te voorkomen (structurele maatregelen). Wanneer het gaat om een beveiligingsincident wordt de vraag welke herstelmaatregelen er moeten worden genomen samen met de ISO beantwoord. Daarbij wordt de CISO geconsulteerd.

De teammanager(s) is/zijn verantwoordelijk voor de uitvoering van de herstelmaatregelen en de structurele maatregelen.

Melding datalek

Als de PO tot de conclusie komt dat er sprake is van een datalek is de PO van de betreffende gemeente verantwoordelijk voor het ‘onverwijld’ doen van de eerste melding bij de AP via het webformulier op de website van de AP. Ondanks dat deze processtap bij alle drie de gemeentes op gelijke wijze wordt ingevuld, blijft elke gemeente individueel aansprakelijk voor het melden van een datalek bij de AP. Wanneer er bijvoorbeeld sprake is van een incident wat alle drie de gemeentes betreft, en dit incident ook gemeld moet worden, dan doen alle drie de PO’s een melding bij de AP voor hun eigen gemeente.

Bij uitbesteding van taken waarbij sprake is van verwerking van persoonsgegevens door verwerkers blijft de desbetreffende gemeente verantwoordelijk voor het melden van een datalek. Er zijn dan ook met alle verwerkers afspraken gemaakt over de gestelde eisen op het gebied van gegevensbescherming en over het onmiddellijk melden van incidenten. In elke verwerkersovereenkomst wordt een vakafdeling van de betreffende gemeente genoemd waar een verwerker incidenten kan doorgegeven. Een medewerker van deze afdeling meldt vervolgens het incident bij de DOWR ICT-servicedesk doormiddel van het hierboven genoemde meldingsformulier. De te doorlopen stappen van de procedure zijn vanaf dat moment niet verschillend van wat hierboven al is beschreven.

De PO van de betreffende gemeente doet de melding bij de AP met behulp van de gegevens die door de gemeentelijke organisatie of de verwerker worden aangeleverd. Er wordt gewerkt conform de meldplicht datalekken van de Autoriteit Persoonsgegevens[1]. Als het gaat om een datalek, dat is ontstaan door een beveiligingsincident, ICT-gerelateerd of niet, is de I-werkorganisatie verantwoordelijk voor het aanleveren van de informatie die de betreffende PO nodig heeft om een melding te kunnen doen.

Als de eerste melding is gedaan, wordt door de desbetreffende PO direct beoordeeld of het nodig is om ook een melding te doen bij betrokkene(n). Wanneer een datalek voor de betrokkene(n) waarschijnlijk ongunstige gevolgen heeft, moet het datalek aan deze betrokkene(n) worden gemeld. Aan de hand van de impact van het datalek en de kans dat die impact optreedt, wordt bepaald of een dergelijke melding nodig is. Daarbij wordt de Functionaris Gegevensbescherming (FG) geraadpleegd. Het kan dus voorkomen dat een datalek wel bij de AP wordt gemeld, maar niet aan betrokkenen, omdat hun persoonsgegevens door bepaalde maatregelen onbegrijpelijk of ontoegankelijk zijn geworden en er dus geen sprake is van ‘waarschijnlijk ongunstige gevolgen’.

Het informeren van betrokkene(n) vindt bij voorkeur op dezelfde dag plaats. Wanneer betrokkenen moeten worden geïnformeerd, stelt de PO de directie, de strategisch communicatieadviseur en de persvoorlichter daarvan op de hoogte. Wanneer er sprake is van een datalek dat is ontstaan door een beveiligingsincident informeert de PO tevens de CISO.

De PO van de betreffende gemeente is vervolgens verantwoordelijk voor de follow-up van de melding. Indien de eerste melding aan de AP niet compleet was, wordt deze door de PO aangevuld.

Communicatie en documentatie

De berichtgeving aan betrokkene(n) is ter beoordeling van de strategisch communicatieadviseur en de persvoorlichter. De berichtgeving moet wel de wettelijk vereiste informatie bevatten. De PO wordt daarom geconsulteerd bij de vraag hoe en wat er naar betrokkene(n) moet worden gecommuniceerd. De PO verstrekt de voor de communicatie benodigde gegevens. Wanneer er sprake is van een datalek, dat is ontstaan door een ICT-gerelateerd beveiligingsincident, wordt ook de CISO geconsulteerd.

De communicatie over een datalek kan worden overgenomen door andere partijen zoals lokale, landelijke of sociale media, eigen medewerkers of ketenpartners. Als gevolg van ruis in de communicatie kan een datalek alsnog onnodig escaleren. Belangrijk is dat de desbetreffende gemeente de regie behoudt over de communicatie van een ernstig datalek dat gemeld is bij het AP en eventueel aan betrokkenen. Bij de uitwerking van de communicatiestrategie door de strategisch communicatieadviseur en de persvoorlichter vindt dan ook afstemming plaats welke doelgroepen of overige partijen worden geïnformeerd over het datalek en op welke wijze. Timing is hierbij van belang. Zeker indien de melding al heeft plaatsgevonden aan betrokkene(n). Via een persbericht stelt de gemeente de media op de hoogte, eventueel aanvullend met een persconferentie voor het stellen van vragen. Deze werkwijze wordt afgestemd op de grootte van het datalek.

Na afsluiting van een incident registreert de PO het incident in de daarvoor ingerichte digitale omgeving, samen met de eventuele ontvangstbevestiging van de melding, en de onderliggende documentatie. Deze registratie is aanvullend op dat wat in de DOWR ICT-servicedesk wordt geregistreerd. In deze servicedesk wordt namelijk vastgelegd wat voor een acties er zijn ondernomen in de periode voor de eventuele vaststelling van een datalek. De PO, of diens vervanger, documenteert daarna in de digitale omgeving de inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent het incident, de gevolgen daarvan, de genomen herstelmaatregelen en de genomen structurele maatregelen. De PO documenteert alleen de voor dit doel noodzakelijke gegevens.

Dit is de laatste stap van de procedure en hiermee is het proces afgerond. In de bijlage is een tabel opgenomen met de rollen en verantwoordelijkheden van de personen die bij deze procedure zijn betrokken.

[1] https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

Bijlage bij Procedure datalekken

Incidenten met betrekking tot persoonsgegevens
handeling ← → beveiliging

		Geen ICT	ICT
Melding incident bij ICT-servicedesk	R = teammanager(s)/ medewerker(s) I = PO/ ISO/ CISO		
Onderzoek en impactanalyse incident	R = PO	R = ISO/PO	R = ISO/PO C = CSERT/ CISO
Ontwerp te treffen maatregelen	R = PO	R = ISO/PO C = CISO	
Uitvoering maatregelen	R = teammanager(s)		
Melding datalek (AP/betrokkene(n))	R = PO C = FG A = B&W I = Directie/ strategisch communicatieadviseur/ persvoorlichter	R = PO C = FG A = B&W I = Directie/ strategisch communicatieadviseur/persvoorlichter/CISO	
Communicatie	R = Directie C = PO S = strategisch communicatieadviseur/persvoorlichter		R = Directie C = PO/CISO S = strategisch communicatieadviseur/per svoorlichter
Documentatie	R = PO A = B&W I = gemeenteraad		

R (*Responsible)*
De persoon die (feitelijk) verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die *accountable* is.

A (*Accountable*)
De persoon die (eind)verantwoordelijk is.

S (*Supportive*)
De persoon die het resultaat ondersteunt.

C (*Consulted*)
De persoon die (mede) richting geeft aan het resultaat. Hij/zij wordt voorafgaand aan beslissingen of acties geraadpleegd.

I (*Informed*)
De persoon die geïnformeerd wordt over de beslissingen.