GEMEENTE BEEMSTER
WERELDERFGOED

ingekomen 14 JAN. 2016

Afdeling Bedrijfsvoering
Team Juridische en Veiligheidszaken

Aan de gemeenteraad

uw brief van	*uw kenmerk*	*ons kenmerk*	*datum*
		1249263	5 januari 2016

onderwerp
Wet meldplicht datalekken

Geachte raadsleden,

Met deze brief geven wij een toelichting op de Wet meldplicht datalekken. Tevens stellen wij u op de hoogte van het proces dat momenteel in Purmerend wordt ingericht om straks te kunnen voldoen aan de eisen die deze wet aan ons stelt.
Desgewenst kunt u bij dit proces aansluiten voor de bestanden waarvoor u als raad verantwoordelijke (in de zin van de Wet bescherming persoonsgegevens) bent; waarover hieronder meer.

Samenvatting
Op 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. Deze wet wijzigt de Wet bescherming persoonsgegevens en loopt vooruit op de komst van de Europese Algemene verordening gegevensbescherming.
De wet introduceert o.a. een meldplicht van meldingsplichtige datalekken bij het College bescherming persoonsgegevens; een hoge boete bij niet naleving van deze meldplicht en een kennisgevingsplicht aan de betrokkene wiens gegevens gelekt zijn.
Om aan de wet te voldoen wordt in Purmerend een proces ingericht. Dit proces draait rondom het meldpunt datalekken en een speciaal voor deze wet geopend mailadres: datalek@purmerend.nl

Wet meldplicht datalekken; een toelichting

Aanleiding indiening wetsvoorstel
Op 1 september 2001 is de Wet bescherming persoonsgegevens in werking getreden. Deze wet vormt de Nederlandse uitwerking van de Europese richtlijn 95/46/EG. In januari 2012 heeft de Europese Commissie een voorstel gedaan voor een Europese – rechtstreeks werkende – Algemene verordening gegevensbescherming (AVG). Deze verordening zal bij zijn inwerkingtreding zowel genoemde Europese richtlijn als de Wet bescherming persoonsgegevens gaan vervangen. Op dít moment is de inwerkingtreding van de AVG gepland in januari 2018.

Hoewel de definitieve tekst van de AVG nog niet bekend is, gaat deze naar verwachting bepalingen bevatten om datalekken te melden aan de nationale toezichthouder (in

bijlage(n): Geen

behandeld door: C. de Haan
telefoonnummer 0299-452492

Nederland: College bescherming persoonsgegevens (Cbp), dat sinds 1 januari de naam Autoriteit persoonsgegevens draagt).
Omdat de Nederlandse regering – mede in het licht van datalekken zoals bij DigiNotar - niet op de inwerkingtreding van de AVG wilde wachten, heeft zij in juni 2013 het wetsvoorstel Wet meldplicht datalekken ingediend. Deze wet omvat wijzigingen in de Telecommunicatie-wet (niet relevant voor de gemeente en wordt hier daarom niet verder besproken) en de Wet bescherming persoonsgegevens.

Wijzigingen in de Wet bescherming persoonsgegevens
De voornaamste wijzigingen die de Wet meldplicht datalekken in de Wet bescherming persoonsgegevens teweeg brengt zijn:
1. een spectaculaire stijging van de maximale door het Cbp op te leggen bestuurlijke boete van € 4500,- (vast bedrag) naar € 820.000,- (jaarlijks te indexeren bedrag).
2. de introductie van een meldplicht aan het Cbp van inbreuken op de beveiliging die ernstige nadelige gevolgen (kunnen) hebben voor de bescherming van persoonsgegevens;
3. de introductie van een kennisgevingsplicht aan de betrokkene wiens persoonsgegevens het betreft, indien "de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer" (artikel 34a, tweede lid Wet bescherming persoonsgegevens);
4. de introductie van de plicht om een overzicht bij te houden van meldingsplichtige datalekken;
5. het benadrukken van de rol van de bewerker bij meldingsplichtige datalekken.

Ad 1. Bestuurlijke boete
Het boetebedrag wordt in de nu voorgestelde tekst van de AVG verhoogd tot een maximale boete van € 1.000.000,-.
Uit de wettekst volgt dat deze boete normaal gesproken pas wordt opgelegd nádat het Cbp een bindende aanwijzing heeft gegeven. Door de wijze van inrichten van het meldingsproces (zie hieronder) en het actief bevorderen van informatiebeveiliging/aandacht voor privacy en permanent monitoren op eventuele datalekken, willen wij voorkomen dat Beemster – uiteraard als Beemster besluit bij het Purmerendse proces aan te haken - onderwerp zal zijn van een bindende aanwijzing c.q. boete.

Ad 2a. Meldingsplichtige inbreuken op de beveiliging/datalekken
Allereerst moet worden vastgesteld wat inbreuken op de beveiliging, kortgezegd: datalekken, zijn. Een datalek is een blootstelling van persoonsgegevens aan verlies of onrechtmatige verwerking. Denk hierbij aan:
- verlies of diefstal van een laptop/usb-stick met daarop persoonsgegevens;
- de hack van/inbraak op een systeem met daarin persoonsgegevens;
- andere vormen van kennisname van persoonsgegevens door onbevoegden, zoals:
- bezorging van een brief op het verkeerde adres;
- snuffelen in dossiers op een bureau door een ander dan degene die er op dat moment aan werkt;
- vermelding van alle geadresseerden van een mail in de aanhef en niet in de bcc.
NB Het lekken van andere gegevens dan persoonsgegevens heet een beveiligingslek. Hierover gaat de Wet meldplicht datalekken dus niet.

Vervolgens moet uit de tekst van de wet geconcludeerd worden dat niet alle datalekken, gemeld moeten worden aan het Cbp. Meldingsplichtig zijn slechts dié datalekken die (kunnen) leiden tot ernstig nadelige gevolgen voor de bescherming van persoonsgegevens.
NB Uiteraard laat dit onverlet dat ook ieder niet-meldingsplichtig datalek er één teveel is en getracht zal worden herhaling hiervan te voorkomen.
Het Cbp heeft inmiddels beleidsregels uitgebracht, waarin nader is uitgewerkt wat moet worden verstaan onder meldingsplichtige datalekken. Kortgezegd zijn datalekken meldingsplichtig als ze gevoelige persoonsgegevens betreffen.

Om bovenstaande voorbeelden weer als uitgangspunt te nemen:
- Het verkeerd bezorgen van een brief is niet meldingsplichtig als de brief de uitnodiging voor het eerstvolgende afdelingsuitje bevat; inclusief de namen en contactgegevens van de organisatoren. Het verkeerd bezorgen van een brief is wél meldingsplichtig als een brief informatie bevat over de korting op een uitkering a.g.v. gepleegde fraude of als de brief informatie bevat over het spijbelgedrag van een kind van de geadresseerde.
- Het hacken van/inbreken op een systeem is niet meldingsplichtig als de gemeente hiermee haar verordeningen publiceert. Het hacken van/inbreken op een systeem is wél meldingsplichtig als het de debiteuren/crediteuren administratie van de gemeente betreft of de toegang tot het DigiD.
- Het snuffelen in een dossier is niet meldingsplichtig als het een dossier met bestemmingsplannen of begrotingen betreft. Het snuffelen in een dossier is wél meldingsplichtig als het medische gegevens van Wmo-cliënten betreft.
- Het zichtbaar vermelden van alle geadresseerden van een mail is niet meldingsplichtig als het de geabonneerden op statistische gegevens betreft. Het zichtbaar vermelden van alle geadresseerden van een mail is wél meldingsplichtig als het de tegenstanders van de komst van een islamitische school betreft.

Ad 2b. Wijze van melden
Allereerst: de meldingsplicht rust op de verantwoordelijke. Volgens de Wet bescherming persoonsgegevens is dit diegene die c.q. het bestuursorgaan dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In de gemeentelijke praktijk zal dit meestal ons college zijn en soms de burgemeester. In een aantal gevallen zal dit echter de raad zijn: denk aan de bestanden met gegevens over de raadsleden of het systeem waarin de persoonsgegevens van de griffiemedewerkers zijn opgeslagen.

Artikel 34a van de Wet bescherming persoonsgegevens stelt sinds 1 januari 2016 dat meldingsplichtige datalekken "onverwijld" moeten worden doorgegeven aan het Cbp. In de beleidsregels heeft het Cbp dit vertaald in een meldingsplicht "uiterlijk 72 uur na de ontdekking van het incident".
NB Het Cbp koppelt de meldingsplicht terecht aan het tijdstip van ontdekking van een datalek. Er kan immers geruime tijd overheen gaan voordat een datalek daadwerkelijk ontdekt wordt.

De melding moet worden gedaan met behulp van een webformulier.

Ad 3. Kennisgevingsplicht aan betrokkene
In aanvulling op de melding aan het Cbp is de verantwoordelijke (voor gemeenten: meestal het college of de burgemeester en soms de raad) soms ook verplicht hiervan kennis te geven aan diegene wiens persoonsgegevens het betreft.

Wanneer moet er niet en wanneer wel kennis gegeven worden?
Geen kennisgevingsplicht
- Een kennisgevingsplicht is niet aan de orde als er passende technische beschermingsmaatregelen genomen zijn waardoor de persoonsgegevens voor onbevoegden ontoegankelijk of onbegrijpelijk zijn; bijvoorbeeld door encryptie. De betrokkene ondervindt dan immers geen nadelige gevolgen van het datalek.
NB Aangezien de techniek steeds verder voortschrijdt, kunnen persoonsgegevens op een gestolen laptop die nu ontoegankelijk zijn, over een jaar wél toegankelijk zijn. In dergelijke gevallen kán er dus nog lang na het voldoen aan de meldingsplicht alsnog ook een kennisgevingsplicht ontstaan. De praktijk zal moeten uitmaken wat in deze als acceptabel en werkbaar voor een verantwoordelijke wordt aangemerkt.
- Een kennisgevingsplicht is evenmin aan de orde als hiervoor zwaarwegende redenen aanwezig zijn. Deze redenen staan genoemd in artikel 43 van de Wet bescherming

persoonsgegevens en zien o.a. op de opsporing van strafbare feiten en de toezicht op de naleving van wettelijke voorschriften.

Wel kennisgevingsplicht
Volgens de wet is er een kennisgevingsplicht als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer. In de richtsnoeren wordt dit vertaald in: gevolgen van materiële of immateriële aard a.g.v. het lekken van persoonsgegevens van gevoelige aard. Zie hierboven onder 2a. voor een aantal voorbeelden van gevoelige persoonsgegevens.

Ad 4. Bijhouden van een overzicht
De wet bepaalt dat het overzicht de volgende gegevens bevat:
- de feiten en gegevens omtrent de aard van het datalek;
- de tekst van de kennisgeving aan de betrokkene als die kennisgeving gedaan is.

Volgens de beleidsregels van het Cbp dient het overzicht 3 doelen:
- het lering trekken uit het datalek en uit de manier waarop dit is afgehandeld;
- het antwoord kunnen geven op vragen van betrokkenen en anderen;
- het bieden van een basis om alsnog aan een betrokkene kennis te kunnen geven van een datalek als dit in eerste instantie niet gedaan is, maar later alsnog moet. Bijvoorbeeld a.g.v. bovengenoemde voortschrijdende techniek.
Deze drie doelen dienen niet alleen het belang van de betrokkene(n), maar ook het belang van de verantwoordelijke om zijn bedrijfsvoering te verbeteren.

Het Cbp introduceert minimale bewaartermijnen voor de gegevens die in het overzicht zijn opgenomen:
- minimaal 3 jaar als er op het moment van ontdekking van het datalek geen kennisgevingsplicht richting de betrokkene is. Het Cbp doet daarbij de suggestie periodiek te evalueren of deze kennisgevingsplicht alsnog ontstaan is;
- minimaal een jaar als een kennisgeving wél heeft plaatsgevonden.

Ad 5. De rol van de bewerker in de Wet meldplicht datalekken
Beemster verwerkt niet alle persoonsgegevens waarover zij beschikt zelf. Denk bijvoorbeeld aan Purmerend die namens Beemster allerlei persoonsgegevens verwerkt. Soms doet Beemster de verwerking wel zelf, maar staan de gegevens niet op de eigen servers, maar elders (in de cloud). In beide gevallen is sprake van een bewerkersconstructie. In het eerste voorbeeld zijn de bestuursorganen van Purmerend voor Beemster bewerker. In het tweede geval is de eigenaar van de computer in de cloud bewerker van de persoonsgegevens.

De wet bepaalt dat de verantwoordelijke ervoor zorgt:
- dat de bewerker de persoonsgegevens die hij voor de gemeente Beemster verwerkt afdoende beveiligt;
- dat er met de bewerker afspraken worden gemaakt over de situatie dat er zich bij de bewerker een datalek voordoet.
Deze afspraken gaan bijvoorbeeld over het tijdstip en de wijze waarop de bewerker een datalek aan de verantwoordelijke doorgeeft. Ook is het mogelijk af te spreken dat de bewerker een datalek aan de verantwoordelijke doorgeeft en tegelijkertijd een eerste (voorlopige) melding ervan doet aan het Cbp. Dat geeft de verantwoordelijke meer tijd om alle gegevens te verzamelen die nodig zijn om bovengenoemd webformulier daarna compleet in te kunnen vullen en op te sturen naar het Cbp.

Inrichting gemeentelijk proces om aan de wet en de daarin opgenomen meldingsplicht/kennisgevingsplicht te voldoen

Hoewel e.e.a. nog in ontwikkeling is – en zéker de eerste tijd na de inwerkingtreding van de wet nog bijgeschaafd zal moeten worden – willen wij hierbij alvast de opzet van het proces met u delen.

De spil in het proces wordt het door de gemeente Purmerend in te richten **meldpunt datalekken**.
Dit meldpunt:
- ontvangt van de diverse Purmerendse/Beemster organisatie-onderdelen, van bewerkers dan wel van burgers en bedrijven signalen over datalekken. Het is aan u om te beslissen of ook de raad één van de leveranciers van de hier bedoelde signalen wil zijn en dus aan wil sluiten bij dit proces c.q. bij het meldpunt datalekken;
- bekijkt of deze signalen zich laten vertalen in meldingsplichtige datalekken;
- doet zo nodig de melding aan het Cbp;
- doet zo nodig een kennisgeving aan de betrokkene;
- houdt het overzicht bij;
- doet een terugkoppeling aan de melders van signalen over wat er met hun signaal gebeurd is;
- houdt in de gaten welke beveiligingstechnische vervolgstappen er genomen worden n.a.v. een gesignaleerd en gemeld datalek, en werkt hier het overzicht op bij.

Voor het doorgeven van signalen van burgers en bedrijven is inmiddels een speciaal mailadres opengesteld: datalek@purmerend.nl . Hieraan zal in de media van (Beemster en) Purmerend aandacht besteed worden. Sowieso zullen wij in de media en op de gemeentelijke website aandacht besteden aan de inwerkingtreding van deze wet.

Het meldpunt datalekken wordt – voorlopig – bemenst door 2 medewerkers van de Purmerendse afdeling Bedrijfsvoering. Om het meldpunt minder kwetsbaar te maken, wordt nog bekeken of dit aantal uit te breiden is naar 4 medewerkers. Na de inwerkingtreding van de AVG gaat de uitvoering van deze taken voor Purmerend naar verwachting over op de Functionaris voor de gegevensbescherming. In Beemster zal dan gekeken moeten worden of de Purmerendse werkwijze overgenomen wordt of dat de taken van het meldpunt datalekken dan overgaan op de Beemster Functionaris voor de gegevensbescherming.

De genoemde maatregelen om op 1 januari 2016 te kunnen voldoen aan de wettelijke meldplicht realiseren wij met beschikbare middelen. Omdat nu nog onduidelijk is met hoeveel meldingen wij te maken krijgen en wat de AVG straks van ons verlangt, kunnen wij op dit moment niet aangeven of er aanvullende financiering nodig is.

Wij zullen u in 2016 op de hoogte blijven houden van ontwikkelingen over dit onderwerp en hopen u voor nu hierover voldoende geïnformeerd te hebben.

Hoogachtend,
burgemeester en wethouders van Beemster

A.J.M. van Beek
burgemeester

E. Kroese-Vrolijks
secretaris