Wet meldplicht datalekken ontrafeld (update 18-01-2016)

Op 4 juni 2015 is de Wet meldplicht datalekken aangenomen en deze wordt opgenomen in de Wbp (Wet bescherming persoonsgegevens). De nieuwe Wet meldplicht datalekken is per 1 januari 2016 in werking getreden. Het betekent nogal wat voor een gemeente en dit document ontrafelt de complexiteit van deze nieuwe wet.

Update: De laatste weken van 2015 en de eerste weken 2016 hebben er nog diverse veranderingen plaats gehad rond de wet meldplicht datalekken. Dit document is een update van het eerder verschenen document "Wetplicht meldplicht datalekken ontrafeld". Hierbij zijn de verplichte meldplicht tijd, de nieuwe boete bedragen en handhavende instantie aangepast.

Is de wet meldplicht datalekken nieuw?
Eigenlijk niet. De Wet datalekken bestaat al langer in Nederland, maar de wet was niet meer up-to-date en de boetebedragen waren zo laag dat niemand zich daar zorgen over maakte. De Europese Commissie heeft alle lidstaten de opdracht gegeven hun wetten aan te passen, zodat voor alle Europese landen dezelfde regels van kracht zijn.

Wat is er veranderd?
Per 1 Januari 2016 is er een verplichte meldplicht waarbij het datalek binnen 72 uur gemeld moet zijn bij de Autoriteit Gegevensbescherming. Bij schending van de meldplicht (EU-regels) wordt standaard een boete opgelegd van € 20.250. Bij naar buiten komen van een datalek waarbij schade is opgelopen, zonder dat een melding is gemaakt door de datalekkende partij aan de Autoriteit Gegevensbescherming, kan een boete oplopen tot € 820.000 of 10 procent van de jaaromzet. De uiteindelijke boete is afhankelijk van de impact van het datalek op de samenleving. De komst van de nieuwe Wet meldplicht datalekken betekent een enorme uitbreiding van de boetebevoegdheid door de Autoriteit Gegevensbescherming.

Wanneer is er sprake van een datalek?
Van een datalek is sprake als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is meestal het gevolg van inbreuk op een of meer beveiligingsmaatregelen. Denk aan recent gepubliceerde voorvallen in de media van uitgelekte medische gegevens of personeelsdossiers die op straat lagen. Ook diefstal van bijvoorbeeld klantgegevens kan een datalek vormen. Elk bedrijf verwerkt (digitale) informatie en dus ook persoonsgegevens, zowel van klanten als medewerkers. Ook de gemeente verwerkt persoonsgegevens, zowel van burgers als van ambtenaren. Door het toenemende risico dat er data wordt 'gelekt', bijvoorbeeld door een menselijke fout, ontoereikende beveiliging, fraude binnen de eigen organisatie en/of een bewuste criminele aanval van buitenaf, kan data in verkeerde handen vallen of verloren gaan. Het wetsvoorstel meldplicht datalekken beoogt aan de huidige Wet bescherming persoonsgegevens (Wbp) een meldplicht voor 'inbreuken op beveiligingsmaatregelen voor persoonsgegevens' toe te voegen.

Hoe zit dat dan met de Wbp?
De Wbp (Wet bescherming persoonsgegevens) bestaat al langer maar wordt de laatste jaren steeds belangrijker, met allerlei nieuwe taken die gemeenten moeten uitoefenen. Daarom eerst een korte uitleg over enkele begrippen uit de Wbp.

De meldplicht gaat gelden voor degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze wordt in de Wbp aangeduid als de 'verantwoordelijke'. Denk bijvoorbeeld aan de volgende situatie: een ambtenaar uit het sociaal domein houdt gegevens van de burger die zorg heeft aangevraagd bij de gemeente in een informatiesysteem. Deze gegevens zijn door het BSN en NAW-gegevens te herleiden tot een individuele burger, dat wil zeggen: een natuurlijke persoon. Deze natuurlijke persoon wordt in de Wbp aangeduid als een 'betrokkene'. De ambtenaar in dit voorbeeld is de verantwoordelijke (eigenlijk is dat het bestuur). Onder persoonsgegevens vallen alle gegevens die herleidbaar zijn tot een geïdentificeerde of identificeerbare natuurlijke persoon (bijv. naam, mailadres, foto, medische gegevens, maar soms óók een IP-adres).
Onder het begrip 'verwerking' valt elke handeling die betrekking heeft op persoonsgegevens, van het moment van verzameling tot vernietiging. Daaronder valt ook het opslaan van gegevens door een derde. Deze derde 'verwerkt' de gegevens in opdracht van de verantwoordelijke en wordt aangeduid als 'bewerker'.

De verplichtingen van de bewerker moeten nauwgezet worden vastgelegd in een bewerkersovereenkomst; dit is een wettelijke vereiste, voortvloeiend uit artikel 14 Wbp. De Autoriteit Gegevensbescherming eist bovendien dat het contract tot in detail vermeldt welke instructies de verantwoordelijke aan de bewerker oplegt, welke beveiliging de bewerker zal toepassen, welke persoonsgegevens verwerkt zullen worden en voor welke doeleinden.

Met de introductie van de nieuwe Wet meldplicht datalekken wordt het nog belangrijker om een adequate en op maat gemaakte bewerkersovereenkomst af te sluiten. Op grond van artikel 13 Wbp is de verantwoordelijke verplicht om passende technische en organisatorische maatregelen ten uitvoer te (laten) leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. De maatregelen moeten bovendien een passend beschermingsniveau garanderen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging en gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

De Autoriteit Gegevensbescherming geeft in 'beleidsregels meldplicht datalekken' aan wanneer er sprake is van een blijvend, passend beveiligingsniveau. Daarin wordt uitgelegd hoe het de Autoriteit Gegevensbescherming bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen deze open beveiligingsnorm uit de Wbp toepast. Daartoe geeft zij een zogeheten 'plan-do-check-act-cyclus' waarin zij allereerst aanraadt om de risico's goed in kaart te brengen en te beoordelen en om gebruik te maken van algemeen geaccepteerde beveiligingsstandaarden. Bovendien adviseert de Autoriteit Gegevensbescherming om regelmatig te controleren en te evalueren. Periodiek dient beoordeeld te worden of het beveiligingsniveau nog steeds past bij de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen. Deze richtsnoeren kunnen verder worden toegepast in samenhang met algemeen geaccepteerde beveiligingsstandaarden binnen het kader van informatiebeveiliging.

Wat zijn de belangrijkste wijzigingen?
De Autoriteit Gegevensbescherming heeft richtsnoeren opgesteld die meer duidelijkheid geven over de daadwerkelijke handhaving van deze wetswijziging. De belangrijkste wijzigingen zijn als volgt:

- Inbreuken op beveiligingsmaatregelen die leiden tot de aanzienlijke kans op ernstige nadelige gevolgen, dan wel ernstige nadelige gevolgen hebben voor de bescherming van persoonsgegevens, moeten door de verantwoordelijke onverwijld worden gemeld bij de Autoriteit Gegevensbescherming;
- Indien de inbreuk waarschijnlijk ongunstige gevolgen heeft voor de betrokkene, moet ook de betrokkene worden geïnformeerd, tenzij de gegevens die gehackt zijn al voldoende versleuteld waren (en niet aannemelijk is dat die beveiliging doorbroken kan worden);
- In bewerkersovereenkomsten moeten afspraken gemaakt worden over de nakoming van alle verplichtingen rondom beveiligingsinbreuken;
- De bestaande boete op schending van de meldplicht of het exportverbod (de EU-regels) wordt verhoogd naar € 20.250;
- Het College Bescherming Persoonsgegevens krijgt de bevoegdheid om op andere delen van de Wet meldplicht datalekken en op de export van persoonsgegevens een bestuurlijke boete op te leggen tot maximaal € 820.000;
- Die hogere boete mag echter alleen worden opgelegd nadat de Autoriteit Gegevensbescherming een bindende aanwijzing aan de overtreder heeft gegeven, tenzij de overtreding opzettelijk is begaan of het gevolg is van ernstige verwijtbare nalatigheid.

Wanneer ben ik in overtreding?
Artikel 66 van de Wbp, waarin de boete, de aanwijzing en de overtredingen beschreven worden, geven de volgende overtredingen aan (samengevat en niet uitputtend):

- Onbehoorlijk verwerken persoonsgegevens;
- Verzamelen zonder doelbinding;
- Verwerken zonder ondubbelzinnige toestemming van de betrokkene;
- Verwerken van op onjuiste gronden verkregen gegevens;
- Doorbreken geheimhoudingsplicht;
- Te lang bewaren van persoonsgegevens;
- Doelbinding en ter zake dienend en niet bovenmatig verwerken;

- Het niet hebben van technische en organisatorische maatregelen met passend beveiligingsniveau;
- Het niet melden van beveiligingsinbreuken;
- Het onjuist melden van incidenten;
- Het niet vastleggen van incidenten;
- Het niet in kennis stellen van de betrokkene;
- Onrechtmatige verwerking bijzondere persoonsgegevens;
- Onrechtmatig verwerken van BSN;
- Het niet aanpassen van gegevens als de betrokkene daar om vraagt;
- Het niet opvolgen van een bindende aanwijzing van de Autoriteit Gegevensbescherming;
- Grove nalatigheid.

Wat moeten gemeenten regelen?

- Noodzaak tot aanpassen van de bewerkersovereenkomst;
- Uitbreiden van bewerkersovereenkomsten: Met de komst van nieuwe taken in het sociaal domein dienen bewerkersovereenkomsten al vanaf begin 2015 in het bezit te zijn van de gemeente. Deze moeten worden uitgebreid met betrekking tot de Wet meldplicht datalekken en aansprakelijkheid.
- Maak richtlijnen over hoe te handelen als zich een datalek voordoet: maak een datalek-draaiboek / -protocol!
- In kaart brengen welke gegevens/datastromen worden verwerkt;
- Toetsen / meten van de huidige informatiebeveiliging op het gebied van datalekken;
- Processen inrichten naar nieuwe regels op gebied van privacy;
- Aanstellen protocolplicht verantwoordelijke;
- Aard en inhoud van de melding vastleggen;
- Kennisgeving aan betrokkenen;
- Zorgdragen dat beveiliging op orde is, zowel technisch als ook organisatorisch;
- Versleutelen van burgergegevens;
- Vooraf inregelen van aspecten rondom beveiliging, datalekken en privacy in een bewerkersovereenkomst en in SLA's (Service Level Agreements).

Wat zijn noodzakelijke acties?

Eigenlijk al het aantoonbare bewijs wat aannemelijk maakt dat uw gemeente er alles aan heeft gedaan dat binnen de mogelijkheden ligt om het datalek te voorkomen. Sommige zaken worden in een project Informatiebeveiliging meegenomen; denk aan monitoring, logging en versleuteling van gegevens. Officieel hoort de wet meldplicht datalekken thuis onder de paraplu van Privacy en nog meer onder Juridische Zaken vanwege het zware juridische karakter.

Wat op korte termijn zeker moet gebeuren is:

- Zorg voor een goede bewerkersovereenkomst met meldplichtpassages en laat deze ondertekenen door de bewerkers vanuit de gemeente;
- Zorg voor een datalekdraaiboek of -protocol zodat ambtenaren weten waarom, wanneer, bij wie en waarin ze een datalek moeten melden en waarbij de protocolplichtverantwoordelijke weet wat er van hem/haar verwacht wordt;
- Datalekken kunt u melden bij het Meldloket Datalekken Autoriteit Gegevensbescherming.

Wat gaat er nog meer veranderen?

- Er komt een EU-wetgeving - ‘Europese Privacy Verordening (EPV)’. Omdat dit een wet is zal de Wbp waarschijnlijk overbodig gaan worden. Als een EU-verordening wordt aangenomen geldt doorgaans een implementatietermijn van twee jaar. We verwachten dat de ingangsdatum van de EU-privacy verordening ergens in 2016 of begin 2017 zou kunnen worden.
- Wat staat nu al vast met deze nieuwe wet:
    - Het recht om vergeten te worden;
    - Een boete van € 1.000.000 of 2% van je jaaromzet;
    - Privacy impact assessments verplicht uitvoeren.

Wat als we niks doen?
Niks doen brengt verhoogde risico's met zich mee. Risico's zijn niet erg als deze bekend zijn binnen de organisatie en de mogelijke impact van het risico bekend is en passende maatregelen genomen zijn. In dit geval betreft het een wet en dit maakt zaken dwingender, zeker voor een gemeente.
U en uw bestuur kunnen als verantwoordelijke aansprakelijk zijn voor alle schade die voortvloeit uit een datalek en daarnaast een boete van de Autoriteit Gegevensbescherming opgelegd krijgen. Om nog maar te zwijgen van de reputatie- en imagoschade en mogelijke claims van betrokkenen!

Welke implicaties heeft dit voor bedrijven en gemeenten? Waar moet een datalek gemeld worden? Wanneer moet een datalek worden gemeld? Wat moet er exact worden gemeld? Welke preventieve maatregelen kunnen er worden getroffen? Welke afspraken kunnen en moeten er met bewerkers worden gemaakt? Op wie rust de meldplicht en wat als er niet - of niet tijdig - wordt gemeld? Al dit soort vragen worden beantwoord in 'beleidsregels meldplicht datalekken' van de Autoriteit Gegevensbescherming.

Meer weten?
Voor meer informatie kunt contact opnemen met John Vloemans, senior adviseur informatiebeveiliging en privacy bij Telengy, via tel. nr. 06 54 34 50 89 of via e-mail: j.vloemans@telengy.nl.